

1990.62597

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re U.S. Patent Application)
)
Applicant: Utsumi et al.)
)
Serial No.)
)
Filed: September 24, 1998)
)
For: STORING APPARATUS)
AND PASSWORD CONTROL)
METHOD)
)
Art Unit:)

I hereby certify that this paper is being deposited with the United States Postal Service as Express Mail in an envelope addressed to: Asst. Comm. for Patents, Washington, D.C. 20231, on this date.

09/24/98

Date

Express Mail/Label No.: EM044996791US

Assistant Commissioner for Patents
Washington, DC 20231

Sir:

CLAIM FOR PRIORITY

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

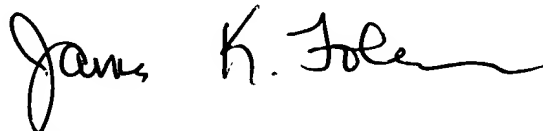
Japanese Patent Application No. 10-065281

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

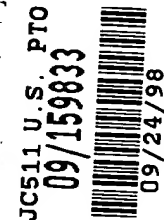
By



James K. Folker

Reg. No. 37,538

September 24, 1998
Sears Tower - Suite 8660
233 South Wacker Drive
Chicago, IL 60606
(312) 993-0080



JC511 U.S. PTO

09/159833



P A T E N T O F F I C E
J A P A N E S E G A V E R N M E N T

This is certify that the annexed is a true copy of the following
application as filed with the Office.

Date of Application : March 16, 1998

Application Number : Patent Application No.Heisei 10-065,281

Applicant (s) : Fujitsu Limited

July 24, 1998

Commissoner, Takeshi Isayama

Patent Office

Certificate No.Hei 10-3056440

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

JCS11 U.S. PTO
09/159833
09/24/98

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application:

1998年 3月16日

願番号
Application Number:

平成10年特許願第065281号

願人
Applicant(s):

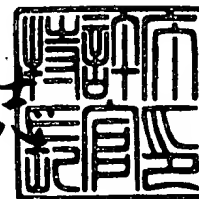
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1998年 7月24日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



出証番号 出証特平10-3056440

【書類名】 特許願

【整理番号】 9800549

【提出日】 平成10年 3月16日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 19/04

【発明の名称】 記憶装置及びそのパスワード制御方法

【請求項の数】 21

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 内海 研一

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 内田 好昭

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小林 弘幸

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100079359

 【弁理士】

 【氏名又は名称】 竹内 進

 【電話番号】 03(3432)1007

【選任した代理人】

 【識別番号】 100093584

【弁理士】

【氏名又は名称】 宮内 佐一郎

【電話番号】 03(3432)1007

【手数料の表示】

【予納台帳番号】 009287

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704823

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 記憶装置及びそのパスワード制御方法

【特許請求の範囲】

【請求項 1】

媒体に記録された情報のアクセスをパスワードにより保護するための記憶装置に於いて、

デフォルト入力パスワード及びアクセス保護用パスワードを保存するパスワード保存部と、

ユーザからのパスワード入力がない場合は、前記デフォルト入力パスワードをユーザ入力パスワードに置き換えて前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、ユーザ入力パスワードと前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御するパスワード検証部と、
を備えたことを特徴とする記憶装置。

【請求項 2】

請求項 1 記載の記憶装置に於いて、前記パスワード保存部で前記デフォルト入力パスワードとアクセス保護用パスワードに同じ値を保存していた場合、前記パスワード検証部は、ユーザのパスワード入力がなくとも、前記デフォルト入力パスワードをユーザ入力パスワードに置き代えたアクセス保護用パスワードとの照合によりアクセスを許可することを特徴とする記憶装置。

【請求項 3】

請求項 1 記載の記憶装置に於いて、前記パスワード保存部は、更にユーザ入力のパスワードを格納するユーザ入力パスワード領域を有し、

前記パスワード検証部は、

電源投入、コマンドリセット、エラーリセット、更に媒体挿入等の装置の使用

【請求項 6】

請求項 1 記載の記憶装置に於いて、

前記パスワード保存部は、前記デフォルト入力パスワードとアクセス保護用パスワードを前記媒体に保存し、

前記パスワード検証部は、装置の使用開始時に前記媒体から前記デフォルト入力パスワードとアクセス保護用パスワードを装置本体に読み出してアクセス保護を制御することを特徴とする記憶装置。

【請求項 7】

請求項 1 記載の記憶装置に於いて、

前記パスワード保存部は、前記デフォルト入力パスワードを装置本体の不揮発性メモリに保存すると共に、前記アクセス保護用パスワードを媒体に保存し、

前記パスワード検証部は、装置の使用開始時に前記媒体から前記アクセス保護用パスワードを装置本体に読み出してアクセス保護を制御することを特徴とする記憶装置。

【請求項 8】

請求項 1 記載の記憶装置に於いて、

前記パスワード検証部は、前記アクセス保護用パスワードを装置本体の不揮発性メモリに保存すると共に、前記デフォルト入力パスワードを媒体に保存し、

前記パスワード処理部は、装置の使用開始時に前記媒体から前記デフォルト入力パスワードを装置本体に読み出してアクセス保護を制御することを特徴とする記憶装置。

【請求項 9】

請求項 5 乃至 7 のいずれかに記載の記憶装置に於いて、前記媒体は通常のリードコマンド及びライトコマンドでアクセスすることのできない特定領域に前記パスワードを保存するパスワード保存領域を設けたことを特徴とする記憶装置。

【請求項 10】

請求項 1 記載の記憶装置に於いて、更に、上位装置からの専用コマンドに基づいて前記デフォルト入力パスワード又は前記アクセス保護用パスワードを書き替えるパスワード書替部を備えたことを特徴とする記憶装置。

【請求項 11】

請求項 5 乃至 7 のいずれかに記載の記憶装置に於いて、前記媒体は装置本体の内部に固定的に収納された媒体であることを特徴とする記憶装置。

【請求項 12】

請求項 5 乃至 7 のいずれかに記載の記憶装置に於いて、前記媒体は装置本体に対し着脱自在なリムーバブル媒体であることを特徴とする記憶装置。

【請求項 13】

請求項 1 記載の記憶装置に於いて、

前記パスワード保存部は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワードを保存し、

前記パスワード検証部は、照合一致が得られたアクセス保護用パスワードの種別に対応した通常コマンドによるアクセスを許可することを特徴とする記憶装置。

【請求項 14】

請求項 13 記載の記憶装置に於いて、

前記パスワード保存部は、アクセス保護用パスワードとして、読出及び書込コマンドによるアクセスを許可する書込読出パスワードと、読出コマンドによるアクセスのみを許可する読出オンリーパスワードとを保存し、

前記パスワード検証部は、前記書込読出パスワードの照合一致が得られた場合は通常の書込コマンド又は読出コマンドによるアクセスを許可し、前記読出オンリーパスワードの照合一致が得られた場合は通常の読出コマンドのみによるアク

セスを許可することを特徴とする記憶装置。

【請求項 15】

請求項 1 記載の記憶装置に於いて、更に、デフォルト入力パスワードに有効期間を設定する有効期間設定部を設けたことを特徴とする記憶装置。

【請求項 16】

請求項 15 記載の記憶装置に於いて、前記有効期間設定部は、装置の使用回数をカウンタで計数し、前記カウンタの値が所定値に達したとき、前記デフォルト入力パスワードをそれまでのデフォルトパスワードとは異なる値に強制的に変更することを特徴とする記憶装置。

【請求項 17】

請求項 15 記載の記憶装置に於いて、前記有効期間設定部は、有効期限の時刻を設定し、装置を使用した際の現在時刻が前記有効期限を超えていたとき、前記デフォルト入力パスワードをそれまでのデフォルトパスワードとは異なる値に強制的に変更することを特徴とする記憶装置。

【請求項 18】

媒体に記録された情報のアクセスをパスワードにより保護するためのパスワード制御方法に於いて、

デフォルト入力パスワード及びアクセス保護用パスワードを保存するパスワード保存過程と、

ユーザからのパスワード入力がない場合は、前記デフォルト入力パスワードをユーザ入力パスワードに置き換えて前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、前記ユーザ入力パスワードと前記アクセス保護用パスワードとの比較照合によりアクセス保護を制御するパスワード検証過程と、

を備えたことを特徴とするパスワード制御方法。

【請求項 19】

請求項 18 記載のパスワード制御方法に於いて、前記デフォルト入力パスワードとアクセス保護用パスワードに同じ値を保存していた場合、前記パスワード検証過程は、ユーザのパスワード入力に先立って、前記デフォルト入力パスワードの値をユーザ入力パスワードに複写して、これとアクセス保護用パスワードを照合することによりアクセスを許可又は不許可することを特徴とするパスワード制御方法。

【請求項 20】

請求項 18 記載のパスワード制御方法に於いて、

前記パスワード保存過程は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワードを保存し、

前記パスワード検証過程は、照合一致が得られたアクセス保護用パスワードの種別に対応した通常コマンドによるアクセスを許可することを特徴とするパスワード制御方法。

【請求項 21】

請求項 18 記載のパスワード制御方法に於いて、更に、デフォルト入力パスワードに有効期間を設定する有効期間設定処理を設けたことを特徴とするパスワード制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンピュータやワードプロセッサ、電子ブック等の情報処理機器に接続するハードディスクドライブや光ディスクドライブ等の記憶装置及びパスワード制御方法に関し、特に、媒体に記録された情報のアクセスをパスワードにより保護するための記憶装置及びパスワード制御方法に関する。

【0002】

【従来の技術】

従来、ハードディスクドライブや光ディスクドライブ等の記憶装置にあっては、パスワードを使用して媒体に記録したデータを保護するようにしている。即ち、記憶装置の媒体に対するデータの読み書きを特定の人にだけ認め、他の人にはアクセスさせないためにパスワードによって本人確認を行っている。

【0003】

例えば、記憶装置あるいは記憶媒体に予めパスワードを書き込んで保存しておき、記憶装置を使用する時にユーザがパスワードを入力し、ユーザ入力のパスワードと装置側に保存したパスワードとが一致すると、記憶媒体への書込コマンド又は読出コマンドを受け付ける。パスワードが不一致であれば書込コマンド又は読出コマンドを受け付けず、エラーを返すものである。

【0004】

このようなパスワードにより個人を認証するシステムは、記憶装置のアクセス保護に限らず、データ通信システムでの端末装置の使用など多くの場合に用いられる。またパスワードを用いた保護システムは、簡単に実装できる技術でありながら、一定の効果を期待できるので広く使われている。

【0005】

【発明が解決しようとする課題】

しかしながら、このようなパスワードを用いたアクセス保護は、広く使われる故に、個々人のユーザは多数のパスワードを持つことになり、全てのパスワードを覚えておくのが困難な場合も多い。このため、ユーザが自分で使用しているパスワードを忘却した場合、正しいユーザであってもアクセスできなくなってしまうという問題がある。

【0006】

そこでユーザはパスワードを手帳などに記録しておき、装置を使う度に手帳のパスワードを確認するといった使い方も見受けられる。これでは、ユーザの手帳を

盗み見ることによってパスワードが知れてしまうという問題がある。

また、パスワードを用いたアクセス保護は、アクセスの度にパスワード入力を促すことを想定しているため、職場の同僚などの第三者がパスワードに接する機会も多い。

【0007】

このような問題は、装置を使用する際に常にパスワードの入力を必要とする操作に伴う問題であり、パスワードでアクセス保護を行いながら、更に、使用者がパスワードを入力する頻度を少なくできるような技術が求められる。

この問題を解決するものとして、任意の使用時点でパスワードを削除してパスワードによるアクセス保護を止め、アクセス保護が必要になれば改めてパスワードを設定する手法が考えられる。即ち、保護が必要な期間だけパスワードを設定してアクセス保護を受ける方法である。

【0008】

しかし、この方法には、次の問題がある。第1に、パスワードを再設定するときに、先のパスワードとは異なるパスワードにしてしまうことが多いので、パスワード管理が繁雑になる。つまり、最新のパスワードが何であったか忘れてしまいがち。第2に、パスワードを再設定する場面が第三者に盗み見られる危険がある。

【0009】

本発明は、このような問題点に鑑みてなされたもので、パスワードによるアクセス保護の機能を損うことなく、使用場面によってはユーザのパスワード入力を必要とすることなくアクセス許容されるようにした記憶装置及びパスワード制御方法を提供することを目的とする。

【0010】

【課題を解決するための手段】

図1は本発明の原理説明図である。

図1(A)は、媒体に記録された情報のアクセスをパスワードにより保護するための本発明が対象とする記憶装置44であり、パスワード保存部45とパスワ

ード検証部 48 を備える。パスワード保存部 45 は、デフォルト入力パスワード 60 及びアクセス保護用パスワードを保存する。

【0011】

パスワード検証部 48 は、ユーザからのパスワード入力がない場合は、デフォルト入力パスワード 60 をユーザ入力パスワード 66 に置き換えてアクセス保護用パスワード 62 との比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、ユーザ入力パスワード 66 とアクセス保護用パスワード 62 との比較照合によりアクセス保護を制御する。

【0012】

特に、パスワード保存部 45 でデフォルト入力パスワード 60 とアクセス保護用パスワード 62 に同じ値を保存していた場合、パスワード検証部 48 は、ユーザのパスワード入力がなくとも、デフォルト入力パスワード 60 をユーザ入力パスワード 66 に置き換えてアクセス保護用パスワード 62 との照合によりアクセスを許可する。

【0013】

このように本発明は、記憶装置側にデフォルト入力パスワードを格納し、ユーザからのパスワード入力がない場合は、デフォルト入力パスワードをユーザ入力パスワードと見做してパスワード検証を行うため、デフォルト入力パスワードとアクセス保護用パスワードを同じ値にしておくことによって、ユーザがパスワード入力しなくともアクセス保護は許可されて通常コマンドによるアクセスができ、ユーザによるパスワード入力を省略できる。

【0014】

パスワード保存部 45 は、更にユーザ入力パスワード 66 を格納するユーザ入力パスワード領域 65 を有し、パスワード検証部 48 は、電源投入、コマンドリセット、エラーリセット、更に媒体挿入等の装置の使用開始時に、デフォルト入力パスワード 60 を読み出してユーザ入力パスワード領域 65 に書き込み、次にユーザ入力パスワード領域 65 のデフォルト入力パスワード 60 とアクセス保護用パスワード 62 とを照合一致に基づいてアクセス許可又は不許可を確立する。

【0015】

アクセス許可確立後は、ユーザのパスワード入力がある毎に、ユーザ入力パスワード領域 65 にユーザ入力パスワード 66 を書き込み、次にアクセス保護用パスワード 62 との照合一致に基づいてアクセス許可又は不許可を確立する。

またユーザがパスワードの入力操作を必ず必要とする形態とした場合、パスワード検証部 48 は、装置の使用開始時に、デフォルト入力パスワード 60 を読み出してユーザ入力パスワード領域 65 に書き込んだ状態でユーザのパスワード入力を待ち、ユーザのパスワード入力があった場合は、ユーザ入力パスワード領域 65 のデフォルト入力パスワード 60 をユーザ入力パスワード 66 で上書きした後にアクセス保護用パスワード 62 との照合比較し、アクセス保護を制御する。

【0016】

勿論、デフォルトパスワードとアクセス保護パスワードが異なる時は、ユーザが正しいアクセス保護パスワードを入力しない限り、アクセスは保護される。

パスワード保存部 45 は、図 1 (A) のように、デフォルト入力パスワード 60 とアクセス保護用パスワード 62 を媒体 52 に保存する。このときパスワード検証部 48 は、装置の使用開始時に媒体からデフォルト入力パスワード 60 とアクセス保護用パスワード 62 を装置内部のワークメモリに読み出してアクセス保護を制御する。

【0017】

またパスワード保存部 45 は、デフォルト入力パスワード 60 とアクセス保護用パスワード 62 を装置本体の不揮発性メモリ 40 に保存してもよい。

更に、パスワード保存部 45 は、デフォルト入力パスワード 60 を装置本体の不揮発性メモリ 40 に保存すると共に、アクセス保護用パスワード 62 を媒体 52 に保存してもよい。この場合、パスワード検証部 48 は、装置の使用開始時に媒体 52 からアクセス保護用パスワード 62 を装置本体のワークメモリに読み出してアクセス保護を制御する。

【0018】

更に、パスワード保存部 45 は、アクセス保護用パスワード 62 を装置本体の不揮発性メモリ 40 に保存すると共に、デフォルト入力パスワード 60 を媒体 52 に保存し、この場合、パスワード検証部 48 は、装置の使用開始時に媒体 52

からデフォルト入力パスワード60を装置本体に読み出してアクセス保護を制御する。

【0019】

媒体52は通常のリードコマンド及びライトコマンドでユーザがアクセスすることのできない特別領域にパスワードを保存するパスワード保存領域68を設ける。これによってパスワードが通常のリードコマンドで読み出されたり、ライトコマンドで書き替えられることを防止する。

更に、上位装置42からの専用コマンドに基づいてデフォルト入力パスワード60又はアクセス保護用パスワード62を書き替えるパスワード書替部54を設ける。媒体は装置本体の内部に固定的に収納された媒体であってもよいし、装置本体に対し着脱自在なりムーバブル媒体であってもよい。

【0020】

パスワード保存部45は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワード62を保存し、パスワード検証部48は、照合一致が得られたアクセス保護用パスワード62の種別に対応した通常コマンドによるアクセスを許可する。

例えばパスワード保存部45は、アクセス保護用パスワード62として、読出及び書込コマンドによるアクセスを許可する書込読出パスワード62と、読出コマンドによるアクセスのみを許可する読出オンリーパスワード64とを保存し、パスワード検証部48は、書込読出パスワード62の照合一致が得られた場合は通常の書込コマンド又は読出コマンドによるアクセスを許可し、読出オンリーパスワード64の照合一致が得られた場合は通常の読出コマンドのみによるアクセスを許可する。

【0021】

更に、デフォルト入力パスワード60に有効期間を設定する有効期間設定部を設ける。このようにパスワード入力を省略できる状態を一定期間だけに限定して継続させることにより、不用意な長期間に亘って無防備な状態が続くことを防止できる。

また逆に一定期間経過後に、パスワードが省略できる状態とする使い方もでき

る。即ち、一定期間後にデフォルトパスワードをアクセス保護パスワードと等しくなるようにすることで、一定期間後にパスワードを入力しなくともアクセスできる状態とすることができる。

【0022】

有効期間設定部は、装置の使用回数をカウンタで計数し、カウンタの値が所定値に達したとき、デフォルト入力パスワード60を異なる値に強制的に変更して使えなくする。また有効期間設定部は、有効期限の時刻を設定し、装置を使用した際の現在時刻が有効期限を超えていたとき、デフォルト入力パスワード60を異なる値に強制的に変更して使えないようにする。

【0023】

また本発明は、媒体に記録された情報のアクセスをパスワードにより保護するためのパスワード制御方法を提供するもので、次の手順から成る。

デフォルト入力パスワード60、アクセス保護用パスワード62及びユーザ入力パスワード66を保存するパスワード保存過程；

ユーザからのパスワード入力がない場合は、デフォルト入力パスワード60をユーザ入力パスワード66に置き換えてアクセス保護用パスワード62との比較照合によりアクセス保護を制御し、ユーザのパスワード入力がある場合は、ユーザ入力パスワード66とアクセス保護用パスワード62との比較照合によりアクセス保護を制御するパスワード検証過程；

とを備える。

【0024】

ここでデフォルト入力パスワード60とアクセス保護用パスワード62に同じ値を保存していた場合、パスワード検証過程は、ユーザのパスワード入力がなくとも、デフォルト入力パスワード60をユーザ入力パスワードに置き換えてアクセス保護用パスワード62との照合によりアクセスを許可する。

またパスワード保存過程は、アクセス保護の種別に応じた複数種類のアクセス保護用パスワード62を保存し、パスワード検証過程は、照合一致が得られたアクセス保護用パスワード62の種別に対応した通常コマンドによるアクセスを許可することを特徴とする。更に、デフォルト入力パスワード60に有効期間を設

定する有効期間設定過程を設ける。これ以外の詳細は装置構成と同じである。

【0025】

【発明の実施の形態】

＜目次＞

1. 固定媒体の記憶装置
2. リムーバブル媒体の記憶装置

1. 固定媒体の記憶装置

図2は本発明のデフォルト入力パスワードを用いたパスワード保護が適用されるハードディスクドライブのブロック図であり、ハードディスクドライブにあつては、磁気ディスク媒体がドライブ本体に固定的に内蔵されている。

【0026】

図2において、ハードディスクドライブ(HDD)はエンクロージャ10とコントロールボード12で構成される。エンクロージャ10にはヘッドIC回路14が設けられ、この実施形態にあつては4つのヘッドアッセンブリ16-1～16-4を接続している。

ヘッドアッセンブリ16-1～16-4にはインダクティブヘッドを用いた記録ヘッドとMRヘッド等を用いた再生ヘッドが設けられている。またエンクロージャ10にはヘッドアクチュエータを駆動するVCM18、及びディスク媒体を回転するスピンドルモータ20が設けられる。

【0027】

エンクロージャ10のヘッドIC回路14に対しては、コントロールボード11側にライトチャネル回路28とリードチャネル回路26が設けられている。ライトチャネル回路28とリードチャネル回路26に対してはハードディスクコントローラ24が設けられ、ハードディスクコントローラ24にはフォーマッタやECC回路等が内蔵されている。

【0028】

ハードディスクコントローラ24はインタフェース回路36に接続され、上位

装置としてのホスト側とのデータ伝送によってホストからのライトデータの供給及びホストに対するリードデータの転送を行っている。このインタフェース回路 36 としては、SCSI インタフェース、ATA インタフェース、ATAPI インタフェース、SIS I 等、適宜のインタフェースを使用することができる。

【0029】

この実施形態にあつては、ディスク媒体の記録方式としてゾーン分割による定密度記録方式（ZC DR）を採用しており、ディスク媒体のシリンダを所定シリンダ数ごとにゾーン分割し、各ゾーンごとに異なった周波数を予め設定している。このため、周波数シンセサイザとして機能する PLL 回路 30 が設けられ、リード動作またはライト動作の際のシリンダアドレスから対応するゾーン周波数をセットすることで、ライトチャネル回路 26 及びリードチャネル回路 28 に対するクロック供給を行う。

【0030】

ハードディスクドライブの全体的な制御はMCU（メインコントロールユニット）22が行う。MCU 22にはバスを介してハードディスクコントローラ 24 及びインタフェース回路 28 が接続され、更にワークメモリとして機能するRAM 38 と不揮発性メモリとして機能するフラッシュROM 40 を接続している。

MCU 22 は、ホストからの各種コマンドを受領して解読し、ハードディスクドライブに対する通常コマンドによる通常リード／ライト指示、及びエンクロージャ 10 に設けている VCM 18 によるヘッド位置決め制御のためのサーボコントローラ 34 に対する制御指示を行う。

【0031】

VCM 18 の駆動によるヘッド位置決め制御を行うため、サーボ復調回路 32 とサーボコントローラ 34 が設けられている。この実施形態にあつては、ディスク媒体のサーボ情報としてデータ面サーボ方式を採用しており、このためリードチャネル回路 26 に対する再生信号からサーボ情報を分離して、サーボ復調回路 32 でヘッド位置情報を復元している。

【0032】

図 3 は、図 2 のコントロールボード 12 に設けた MCU 22 のプログラム制御

によって実現されるパスワードを用いた本発明によるアクセス保護の機能ブロック図である。

図3において、上位装置42に対する外部記憶装置としてハードディスクドライブ44が接続されている。ハードディスクドライブ44の不揮発性メモリ40には、この実施形態にあつてはパスワード保存領域45が設けられ、このパスワード保存領域45の中にデフォルト入力パスワード(DPW)60、書込読出パスワード(PA0)62、及び読出オンリーパスワード(PA1)64を保存している。またRAMを用いたワークメモリ38にはユーザ入力パスワード(UPW)66を格納するためのユーザ入力パスワード格納領域65が設けられている。

【0033】

ここで不揮発性メモリ40に格納した書込読出パスワード62及び読出オンリーパスワード64は、上位装置42からのユーザ入力によるユーザ入力パスワード66との照合によりパスワード照合一致が得られた時に、各パスワードで定められたアクセスを許容するアクセス保護用のパスワードである。

即ち書込読出パスワード62は、ユーザ入力パスワード66との照合一致が得られた時に、ディスク媒体52に対する通常のライトコマンドによる書込アクセスまたは通常のリードコマンドによるリードアクセスを許可する。これに対し読出オンリーパスワード64は、ユーザ入力パスワード66との照合一致が得られた時に、ディスク媒体52に対する通常のリードコマンドによる読出アクセスのみを許容する。即ち書込読出パスワード62及び読出オンリーパスワード64は、アクセス保護と同時にアクセス種別を決めるパスワード機能を持っている。

【0034】

このようなアクセス保護用の書込読出パスワード62と読出オンリーパスワード64を用いたアクセス保護は、従来のパスワードを用いたアクセス保護と同じであるが、これに加えて本発明にあつては、新たにデフォルト入力パスワード60を保存している。

デフォルト入力パスワード60は、上位装置42からユーザ入力パスワード66を受けなくともハードディスクドライブ44におけるディスク媒体52のアク

セスを許可するパスワードである。具体的には、ハードディスクドライブ44の使用開始時に上位装置42からユーザによるパスワード入力があった場合には、不揮発性メモリ40に保存しているデフォルト入力パスワード60をユーザ入力パスワード66とみなして、アクセス保護用パスワードである書込読出パスワード62及び読出オンリーパスワード64との比較照合を行う。

【0035】

この比較照合により、デフォルト入力パスワード60が例えば書込読出パスワード62に一致すれば、書込読出パスワード62で指定されるアクセス種別として通常コマンドによる書込アクセス及び読出アクセスを許可する。このようなデフォルト入力パスワード60を用いたアクセス保護を行うため、ハードディスクドライブ44には、コマンド処理部46、パスワード検証部48及びアクセス実行部50が設けられている。

【0036】

コマンド処理部46は、上位装置42からのコマンドを受信して解読し、必要な処理を行う。例えば装置の使用開始時には、ユーザがパスワードを入力すると、ユーザが入力したパスワードがパスワード転送コマンドによりハードディスクドライブ44に送られることから、このパスワード転送コマンドをコマンド処理部46で解読し、コマンドパラメータとして取得したユーザ入力パスワード66をワークメモリ38のユーザ入力パスワード格納領域65に書き込む。

【0037】

またコマンド処理部46にはパスワード書替部54が設けられており、不揮発性メモリ40に格納されているデフォルト入力パスワード60、書込読出パスワード62及び読出オンリーパスワード64の書替えを、上位装置42に対するインタフェースでサポートされるパスワード書替専用のコマンドにより書替え変更ができる。このパスワード書替えコマンドとしては、例えばSCSIインタフェースであればフォーマットコマンドやベンダユニークコマンドが使用できる。

【0038】

パスワード検証部48には、パスワード照合部56とアクセスモード設定部58が設けられる。パスワード照合部56は、ハードディスクドライブ44の使用

開始時に、まず不揮発性メモリ 40 からデフォルト入力パスワード 60 を読み出してワークメモリ 38 のユーザ入力パスワード格納領域 65 に書き込む。このため装置使用開始時に、まずユーザ入力パスワード 66 としてはデフォルト入力パスワード 60 の値がセットされる。

【0039】

ワークメモリ 38 のユーザ入力パスワード格納領域 65 にユーザ入力パスワード 66 としてデフォルト入力パスワード 60 を書き込んだ後の処理は、次の 2 つがある。

①ユーザのパスワード入力を待たずにパスワード照合を行う処理

②ユーザのパスワード入力の実行操作を待ってパスワード照合を行う処理

まずユーザのパスワード入力を待たない処理にあっては、ワークメモリ 38 のユーザ入力パスワード格納領域 65 に対するデフォルト入力パスワード 60 の書き込みが済むと、ワークメモリ 38 からユーザ入力パスワード 66 と不揮発性メモリ 40 から書込読出パスワード 62 を読み出し、両者を照合する。

【0040】

このパスワード照合で照合一致が得られると、書込読出パスワード 62 で決まるアクセスモードをアクセスモード設定部 58 で設定し、アクセス実行部 50 に対し上位装置 42 からの通常のライトコマンドによる書込アクセス及びリードコマンドによる読出アクセスの許可状態を確立する。

一方、上位装置 42 からのユーザによるパスワード入力操作を待つ処理にあっては、パスワード照合部 56 でワークメモリ 38 のユーザ入力パスワード格納領域 65 にデフォルト入力パスワード 60 を書き込んだ後、上位装置 42 からのパスワード転送コマンドの受信を待つ。

【0041】

コマンド処理部 46 でパスワード転送コマンドが受信されると、コマンドパラメータとして受信したパスワードをワークメモリ 38 のユーザ入力パスワード格納領域 65 に上書きし、上書き後のユーザ入力パスワード 66 と不揮発性メモリ 40 の書込読出パスワード 62 をパスワード照合部 56 に読み出して照合し、照合一致が得られればアクセスモード設定部 58 で書込読出モードをアクセスモー

ドとして設定する。

【0042】

この場合、本発明にあっては、上位装置42でユーザがパスワードの文字列を入力することなくパスワードの入力欄を空欄としたままパスワード入力を実行した場合については、実質的にユーザ入力パスワードの文字列が受信されなくとも、デフォルト入力パスワード60に基づいたアクセス許可状態を確立する。

即ち、コマンド処理部46で上位装置からパスワード転送コマンドを受信しても、コマンドパラメータとしてのパスワードの文字列が空文字列であった場合、パスワード照合部56は既にデフォルト入力パスワード60に書き替えられているユーザ入力パスワード66を読み出して不揮発性メモリ40の書込読出パスワード62と照合し、照合一致が得られれば、書込読出モードをアクセスモードとしてアクセスモード設定部58により設定させる。

【0043】

ここでハードディスクドライブ44のパスワード検証部48が不揮発性メモリ40のデフォルト入力パスワード60に基づいたアクセス保護を行う装置使用開始タイミングの内容としては、

- ①ハードディスクドライブ44の電源投入時
- ②上位装置42とのインタフェースによりコマンドリセットが行われた時
- ③ハードディスクドライブ44が重大なエラー状態となり、内部リセットにより復帰した時

等がある。

【0044】

図4は、図3のユーザのパスワード入力を必要としないアクセス保護の処理動作である。まず図3の不揮発性メモリ40に保存されているデフォルト入力パスワード60、書込読出パスワード62及び読出オンリーパスワード64は、ハードディスクドライブ44を低レベルフォーマットである初期化時に、予め定めた規定値、例えばオール0に初期化されている。

【0045】

図4のハードディスクドライブ44は、初期化状態にあるデフォルト入力パス

ワード60及び書込読出パスワード62であり、各パスワードは16進で「0000000h」となっている。尚、図5には示していない図3の読出オンリーパスワード64も同じ「00000000h」となっている。

このようなデフォルト入力パスワード60及び書込読出パスワード62が初期化により同じ値で保存された状態で、ハードディスクドライブ44の電源が投入されたとすると、ハードディスクドライブ44側において図3のパスワード検証部48が、まずデフォルト入力パスワード60を読み出して、空き状態にあるユーザ入力パスワード格納領域65にユーザ入力パスワード66として書き込む書込み処理70を行う。

【0046】

次にデフォルト入力パスワード60の値が書き込まれたユーザ入力パスワード66と書込読出パスワード62を読み出して照合比較処理72を実行する。この場合、ユーザ入力パスワード66は、デフォルト入力パスワード60の書込処理70によって書込読出パスワード62と同じ値となっており、照合一致が得られることで書込読出モードとなるアクセス許可74が行われる。

【0047】

図4は、デフォルト入力パスワード60及び書込読出パスワード62の値を初期化による「00000000h」とした場合を例にとっているが、ハードディスクドライブ44がアクセス許可を確立して書込及びまたは読出アクセスが可能となった後は、上位インタフェースからのパスワード書替コマンドによってデフォルト入力パスワード60及び書込読出パスワード62、更には読出オンリーパスワード64の値を別の値に書き替えることができる。このパスワードの書替えは、図3に示したコマンド処理部46のパスワード書替部54により行われる。

【0048】

図5は、図3のパスワード書替部54によるパスワード書替処理である。まず上位装置42側より書込読出パスワード（アクセス保護パスワード）62の書替コマンドを発行する。この書込読出パスワード62の書替コマンドは、例えば「Change Password 0“0F1E2D3C”」となる。この書替コマンドにより、図4の書込読出パスワード62の値「00000000h」は、

図6の書替え処理76によって「0F1E2D3Ch」に書き替えられる。

【0049】

このように書込読出パスワード62を書き替えた場合には、ユーザのパスワード入力を必要としないアクセス許可を確立するため、デフォルト入力パスワード60についても書込読出パスワード62と同じ値に書き替える。このデフォルト入力パスワード60の書替コマンドは例えば「Change Default Psw "0F1E2D3C"」であり、書替み処理78により図示のように書込読出パスワード62と同じ値に書き替えられる。

【0050】

尚、設定済みのデフォルト入力パスワードに併せてアクセス保護パスワードを書替えてもよい。

このようにデフォルト入力パスワード60及びアクセス保護パスワードとしての書込読出パスワード62を別の値に書き替えた後についても、ハードディスクドライブ44が再度使用開始となれば、上位装置42でユーザがパスワードを入力しなくとも、デフォルト入力パスワード60の値を書込処理80によりユーザ入力パスワード66として書き込み、次にデフォルト入力パスワード60を書き込んだユーザ入力パスワード66と書込読出パスワード62との照合比較処理82を行い、この場合もパスワードは一致することから、書込読出アクセスのアクセス許可84を確立する。

【0051】

勿論、正しいパスワードを入力しない時にアクセスを禁止したい場合には、図4の初期化によるオール0となっているデフォルト入力パスワード60と書込読出パスワード62のいずれか一方を別の値に書き替えれば良く、デフォルト入力パスワード60と書込読出パスワード62が異なれば照合一致処理で不一致となることからアクセス許可は得られず、書込読出パスワード62に一致するユーザのパスワード入力のみによってアクセス許可を確立することができる。

【0052】

図6は、図3のパスワード検証部48に設けたアクセスモード設定部58で確立されるハードディスクドライブ44のアクセスモードとアクセス内容である。

即ち、アクセスモードは書込読出モード、読出オンリーモード及びセキュリティモードの3つとなり、書込読出モードは通常の読出コマンドと書込コマンドを受け付ける。またデフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードの変更を許可する。

【0053】

読出オンリーモードは、通常の読出コマンドのみを受け付ける。この場合にも、デフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードの変更を許可する。更にセキュリティモードは、通常の読出コマンドと書込コマンドによるアクセスは一切不可とするが、パスワード入力を伴う読出コマンドまたは書込コマンドは受け付ける。もちろん、パスワード照合一致が得られて初めて各コマンドに対するアクセス許可が行われる。

【0054】

ここで図3の実施形態にあっては、ハードディスクドライブ44の不揮発性メモリ40にデフォルト入力パスワード60、書込読出パスワード62及び読出オンリーパスワード64を保存した場合であるが、本発明の他の実施形態として各パスワードを全て磁気ディスク媒体52に格納しても良いし、ハードディスクドライブ44の不揮発性メモリ40と磁気ディスク媒体52に分けて保存するようにしても良い。

【0055】

図7は、本発明のハードディスクドライブ44におけるパスワードの保存形態を表している。保存形態1は図3の実施形態であり、デフォルト入力パスワード及びアクセス保護用のパスワードは共にハードディスクドライブ44側に格納している。保存形態2はデフォルト入力パスワード及びアクセス保護用のパスワードを全て磁気ディスク媒体52に格納した場合である。

【0056】

保存形態3はデフォルト入力パスワードをハードディスクドライブ44側に格納し、アクセス保護用のパスワードについては磁気ディスク媒体52側に格納した場合である。更に保存形態4はデフォルト入力パスワードを磁気ディスク媒体52に保存し、アクセス保護用のパスワードはハードディスクドライブ44に格

納した場合である。この保存形態 2, 3, 4 を具体的に説明すると、図 8, 図 10, 図 11 のようになる。

図 8 は図 7 の保存形態 2 であり、磁気ディスク媒体 52 のパスワード格納領域 68 にデフォルト入力パスワード 60、書込読出パスワード 62 及び読出オンリーパスワード 64 を保存している。このためハードディスクドライブ 44 の使用開始時には、パスワード検証部 48 がアクセス実行部を経由して磁気ディスク媒体 52 からデフォルト入力パスワード 60、書込読出パスワード 62 及び読出オンリーパスワード 64 を読み出してワークメモリ 38 のパスワード格納領域 67 に展開する。またワークメモリ 38 にはユーザ入力パスワード 66 を格納するためのユーザ入力パスワード格納領域 65 が確保されている。

【0057】

図 9 は図 8 の磁気ディスク媒体 52 のパスワード保存状態である。この実施形態にあっては、磁気ディスク媒体の論理ブロックアドレス $LBA = 1$ が通常のリードコマンドまたはライトコマンドでアクセスすることのできないディスク管理領域 70 に割り当てられていることから、ディスク管理領域 70 の中の専用領域としてパスワード保存領域 68 を確保し、ここにデフォルト入力パスワード 60、読出オンリーパスワード 64 及び書込読出パスワード 62 を保存している。

【0058】

図 10 は図 7 の保存形態 3 であり、ハードディスクドライブ 44 側となる不揮発性メモリ 40 に確保したパスワード格納領域 45 にデフォルト入力パスワード 60 を保存し、一方、磁気ディスク媒体 52 のパスワード格納領域 68 にはアクセス保護用の書込読出パスワード 62 と読出オンリーパスワード 64 を保存している。

【0059】

このため、ワークメモリ 38 にはパスワード格納領域 67 が確保されており、ハードディスクドライブ 44 の使用開始時にアクセス検証部 48 はアクセス実行部 50 を介して、まず磁気ディスク媒体 52 のパスワード格納領域 68 から読出オンリーパスワード 62 及び読出オンリーパスワード 64 を読み出してワークメモリ 38 に展開する。もちろんワークメモリ 38 には、ユーザ入力パスワード 6

6を格納するためのユーザ入力パスワード格納領域65も確保されている。

【0060】

図11は図7の管理モード4の実施形態であり、この実施形態にあっては、磁気ディスク媒体52のパスワード格納領域68にデフォルト入力パスワード60を保存し、一方、ハードディスクドライブ44の不揮発性メモリ40に設けたパスワード保存領域45にはアクセス保護用の書込読出パスワード62と読出オンリーパスワード64を保存している。

【0061】

またワークメモリ38にはパスワード格納領域67が確保され、ハードディスクドライブ44の使用開始時にアクセス検証部48は、まずアクセス実行部50を介して磁気ディスク媒体52のパスワード格納領域68からデフォルト入力パスワード60を読み出して、ワークメモリ38に図示のように展開する。

尚、図8、図10及び図11の保存形態2、3、4のそれぞれにおけるハードディスクドライブ44に設けているコマンド処理部46、パスワード検証部48、アクセス実行部50、パスワード書替部54、パスワード照合部56、アクセスモード設定部58の処理機能は、図3の保存形態1の実施形態と同じである。

【0062】

図12は、ハードディスクドライブ44を対象とした本発明のアクセス保護におけるユーザのパスワード入力を必要としないアクセス保護処理のフローチャートである。この処理を例えば図3の保存形態1の実施形態を例にとって説明すると次のようになる。

ハードディスクドライブ44の電源投入、運用中におけるインタフェースのリセットコマンド、更には重大エラーからの内部リセット等を受けてハードディスクドライブ44の使用が開始されると、まずステップS1でデフォルト入力パスワード60を読み出してユーザ入力パスワード格納領域65に書き込む設定処理を行う。続いてステップS2でデフォルト入力パスワード60に書き替えられたユーザ入力パスワード66と書込読出パスワード62を比較照合する。

【0063】

このとき図4のようにユーザ入力パスワード66と書込読出パスワード62が

同じ値であれば、ステップ S 3 で照合一致が判別され、ステップ S 6 で書込読出モードが確立される。一方、ステップ S 3 でデフォルト入力パスワード 60 で書き替えたユーザ入力パスワード 66 が書込読出パスワード 62 に不一致であった場合には、ステップ S 4 で読出オンリーパスワード 64 とデフォルト入力パスワード 60 で書き替えられたユーザ入力パスワード 66 の比較照合を行う。

【0064】

この比較照合でステップ S 5 で照合一致が判別されると、ステップ S 7 で、この場合には読出オンリーモードが設定される。一方、ステップ S 5 においても照合不一致となった場合には、ステップ S 8 のセキュリティモードに進み、通常のリードコマンドあるいはライトコマンドによるアクセスは一切禁止し、ユーザのパスワード入力に伴うアクセスのみを受け付けることになる。

【0065】

図 13 は、ユーザがパスワードを入力した場合のアクセス保護処理のフローチャートである。このユーザがパスワードを入力した場合の処理は、図 12 のステップ S 8 でセキュリティモードに入った状態、あるいは装置使用開始時にユーザがパスワードを入力した場合、更には運用中の適宜のタイミングのいずれにおいても、ユーザによるパスワード入力があれば実行される処理となる。

【0066】

まずユーザのパスワード入力に伴うパスワード転送コマンドを受信すると、ステップ S 1 で、ユーザが入力したパスワードをワークメモリ 38 のユーザ入力パスワード格納領域 65 にユーザ入力パスワード 66 として設定する。次にステップ S 2 でユーザ入力パスワード 66 と書込読出パスワード 62 を比較照合する。

ステップ S 3 で照合一致が得られれば、ステップ S 6 の書込読出モードを設定する。不一致であれば、ステップ S 4 で読出オンリーパスワードと比較照合し、ステップ S 5 で照合一致が得られれば、ステップ S 7 の読出オンリーモードを設定する。ステップ S 5 でも照合不一致であった場合には、ステップ S 8 のセキュリティモードを設定し、通常コマンドによるアクセスは一切禁止する。

【0067】

図 14 は、ハードディスクドライブ 44 を対象とした本発明のアクセス保護の

他の実施形態のフローチャートであり、このフローチャートにあつては、必ずユーザによるパスワード入力操作を必要とする。図14の処理を図3の保存形態1の実施形態を例にとって説明すると、次のようになる。

ハードディスクドライブ44の電源投入等により装置の使用が開始されると、まずステップS1でデフォルト入力パスワード60を読み出してユーザ入力パスワード領域65にユーザ入力パスワード66として設定する。続いてステップS2でユーザのパスワード入力を待つ。ユーザのパスワード入力操作の実行でパスワード転送コマンドが受信されると、ユーザのパスワード入力ありを判別してステップS3に進み、ユーザが入力したパスワードは空き文字列か否かチェックする。

【0068】

ユーザが入力したパスワードに正常に文字列が格納されていた場合には、ステップS4に進み、ユーザが入力したパスワードをユーザ入力パスワード領域65に上書きする。一方、ユーザが入力したパスワードが空き文字列であった場合には、ステップS4の上書きは行わず、ステップS1で書き込んだデフォルト入力パスワード60の値をそのままユーザ入力パスワード66として残す。

【0069】

続いてステップS5でユーザ入力パスワード66と書込読出パスワード62を比較照合し、ステップS6で照合一致が得られれば、ステップS9で書込読出モードを設定する。照合不一致であれば、ステップS7でユーザ入力パスワード66と読出オンリーパスワード62を比較照合し、ステップS8で照合一致が得られれば、ステップS10で読出オンリーモードを設定する。照合不一致であれば、ステップS11でセキュリティモードを設定し、通常コマンドによるアクセスを禁止する。

【0070】

この図14の処理にあつては、ユーザがパスワードの文字列を入力せずにパスワード入力の実行操作のみを行った場合、ユーザが入力したパスワードの空き文字列を認識してユーザ入力パスワードの代わりにデフォルト入力パスワードを使用した比較照合が行われ、実質的にユーザはパスワードの文字列を必要とするこ

となく、ハードディスクドライブ44のアクセス可能状態を確立することができる。

2. リムーバブル媒体の記憶装置

図15は本発明が適用されるリムーバブル媒体を用いた記憶装置である光磁気ディスクドライブの回路ブロック図である。勿論、本実施形態は、リムーバブル磁気ディスクや相変化型光ディスク等の可換記憶装置にそのまま適用できる。光ディスクドライブは、コントロールボード110とエンクロージャ111で構成される。

【0071】

コントロールボード110には光磁気ディスクドライブの全体的な制御を行うMCU12、ワークメモリとなるRAM106、不揮発性メモリとなるフラッシュROM108、上位装置との間でコマンド及びデータのやり取りを行うインタフェース117、光ディスク媒体に対するデータのリード・ライトに必要な処理を行う光磁気ディスクコントローラ(ODC)114、DSP116、及びバッファメモリ118が設けられる。

【0072】

光磁気ディスクコントローラ114には、フォーマッタ114-1とECC処理ユニット114-1が設けられる。ライトアクセス時には、フォーマッタ114-1がNRZライトデータを媒体のセクタ単位に分割して記録フォーマットを生成し、ECC処理ユニット114-1がセクタライトデータ単位にECCコードを生成して付加し、更に必要ならばCRCコードを生成して付加する。

【0073】

更に、ECCエンコードの済んだセクタデータを例えば1-7RLL符号に変換する。リードアクセス時には、復調されたセクタリードデータを1-7RLL符号から逆変換し、ECC処理ユニット114-2でCRCチェックした後にエラー検出訂正し、更にフォーマッタ114-1でセクタ単位のNRZデータを連結してNRZリードデータのストリームとし、上位装置に転送させる。

【0074】

光ディスクコントローラ 114 に対してはライト LSI 回路 120 が設けられ、ライト LSI 回路 120 にはライト変調ユニット 121 とレーザダイオード制御回路 122 が設けられる。レーザダイオード制御回路 122 の制御出力は、エンクロージャ 111 側に設けたレーザダイオードユニット 130 に与えられている。レーザダイオードユニット 130 はレーザダイオード 130-1 とモニタ用ディテクタ 130-2 を一体に備える。ライト変調ユニット 121 は、ライトデータを PPM 記録または PWM 記録のでデータ形式に変換する。

【0075】

レーザダイオードユニット 130 を使用して記録再生を行うリムーバブル媒体として光磁気記憶媒体を使用する。媒体の記録フォーマットはゾーン CAV である。更に、媒体の記録方式は、媒体上のマークの有無に対応してデータを記録するピットポジション記録（PPM 記録）、又はマークのエッジ即ち前縁と後縁をデータに対応させるパルス幅記録（PWM 記録）を採用している。

【0076】

光ディスクドライブに MO カートリッジ媒体をローディングした際には、まず媒体の ID 部をリードし、そのピット間隔から MCU 112 において媒体の種別を認識し、種別結果をライト LSI 回路 120 に通知する。

光ディスクドライブ 114 からのセクタライトデータは、ライト変調ユニット 121 で PWM 記録データに変換される。そしてライト変調ユニット 121 で変換された PWM 記録データは、レーザダイオード制御ユニット 122 に与えられ、レーザダイオード 130-1 の発光駆動で媒体に書き込まれる。

【0077】

光ディスクドライブ 114 に対するリード系統としては、リード LSI 回路 124 が設けられ、リード LSI 回路 124 にはリード復調ユニット 125 と周波数シンセサイザ 126 が内蔵される。リード LSI 回路 124 に対しては ID/MO 用ディテクタ 132 からレーザビームの媒体戻り光の受光信号が、ヘッドアンプ 34 を介して ID 信号及び MO 信号として入力されている。

【0078】

リード LSI 回路 124 のリード復調ユニット 125 には、AGC 回路、フィ

ルタ、セクタマーク検出回路等の回路機能が設けられ、入力したID信号及びMO信号よりリードクロックとリードデータを作成し、PWM記録データを元のNRZデータに復調している。

またスピンドルモータ40の制御としてゾーンCAVを採用していることから、MCU112からリードLSI回路124に内蔵した周波数シンセサイザ126に対しゾーン対応のクロック周波数を発生させるための分周比の設定制御が行われている。周波数シンセサイザ126はプログラマブル分周器を備えたPLL回路であり、媒体のゾーン位置に応じて予め定めた固有の周波数をもつ基準クロックをリードクロックとして発生する。

【0079】

リードLSI124で復調されたリードデータは、光ディスクコントローラ114に与えられ、1-7RLL符号の逆変換後にECC処理ユニット114-2のエンコード機能によってCRDチェックとECC処理を受けてNRZセクタデータが復元され、フォーマッタ114-1でNRZリードデータのストリームに繋げた後に、バッファメモリ118を経由して上位インタフェース117により上位装置に転送される。

【0080】

MCU112に対しては、DSP116を経由してエンクロージャ111側に設けた温度センサ136の検出信号が与えられ、装置内部の環境温度に基づき、レーザダイオード制御ユニット122におけるリード、ライト、イレーズの各発光パワーを最適値に制御する。

MCU112は、DSP116を経由してドライバ138によりスピンドルモータ40を制御し、例えば6000rpmの一定速度で回転させる。またMCU112は、DSP116からドライバ142を介してエンクロージャ111側に設けた電磁石に通電し媒体に記録磁場を与える。

【0081】

DSP116は、媒体に対しレーザダイオード130からのビームの位置決めを行うためのサーボ機能を備え、目的トラックにシークしてオントラックするためのシーク制御を行う。このシーク制御は、MCU112による上位コマンドに

対するライトアクセス又はリードアクセスに並行して同時に実行することができる。

【0082】

DSP116のサーボ機能を実現するため、エンクロージャ111側の光学ユニットに媒体からのビーム戻り光を受光するFES用ディテクタ145を設け、FES検出回路（フォーカスエラー信号検出回路）146が、FES用ディテクタ45の受光出力からフォーカスエラー信号E1を作成してDSP116に入力している。

【0083】

またエンクロージャ111側の光学ユニットに媒体からのビーム戻り光を受光するTES用ディテクタ147を設け、TES検出回路（トラッキングエラー信号検出回路）148がTES用ディテクタ47の受光出力からトラッキングエラー信号E2を作成し、DSP116に入力している。トラッキングエラー信号E2はTZC検出回路（トラックゼロクロス検出回路）150に入力され、トラックゼロクロスパルスE3を作成してDSP115に入力している。

【0084】

エンクロージャ111側には、媒体に対しレーザビームを照射する対物レンズのレンズ位置を検出するレンズ位置センサ152が設けられ、そのレンズ位置検出信号（LPOS）E4をDSP116に入力している。更にDSP116は、媒体上のビームスポットの位置を制御するため、ドライバ158、162、166を介してフォーカスアクチュエータ160、レンズアクチュエータ164及びVCM168を制御駆動している。

【0085】

ここで光ディスクドライブにおけるエンクロージャ11の概略は図16のようになる。ハウジング167内にはスピンドルモータ140が設けられ、スピンドルモータ140の回転軸のハブに対しインレットドア169側よりMOカートリッジ170を挿入することで、内部のMO媒体172がスピンドルモータ140の回転軸のハブに装着されるローディングが行われる。

【0086】

ローディングされたMOカートリッジ170のMO媒体172の下側には、VCM168により媒体トラックを横切る方向に移動自在なキャリッジ176が設けられている。キャリッジ176上には対物レンズ180が搭載され、固定光学系178に設けているレーザダイオードからのビームをプリズム182を介して入射し、MO媒体172の媒体面にビームスポットを結像している。

【0087】

対物レンズ180は図15のエンクロージャ111に設けたフォーカスアクチュエータ160により光軸方向に移動制御され、またレンズアクチュエータ164により媒体トラックを横切る半径方向に例えば数十トラックの範囲内で移動することができる。

図17は、図15の光ディスクドライブを対象とした本発明のデフォルト入力パスワードを用いたアクセス保護の実施形態であり、この実施形態にあつては、図7の保存形態2に従ってデフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードを記憶媒体に保存したことを特徴とする。

【0088】

図17において、MO媒体172の通常コマンドでは読み出し不可の領域にはパスワード格納領域182が設けられ、ここにデフォルト入力パスワード60、書込読出パスワード62及び読出オンリーパスワード64を格納している。またワークメモリ106にはユーザ入力パスワード格納領域202が設けられ、ここにユーザ入力パスワード66を格納している。

【0089】

光ディスクドライブ90にMOカートリッジ170を挿入すると、ワークメモリ160のパスワード格納領域200に図示のようにデフォルト入力パスワード60、書込読出パスワード62及び読出オンリーパスワード64が読み出され、コマンド処理部92、パスワード検証部94及びアクセス実行部96によるアクセス保護処理を受けることになる。

【0090】

デフォルト入力パスワードを用いたアクセス保護のため光ディスクドライブ90には、コマンド処理部92、パスワード検証部94及びアクセス実行部96が

設けられる。パスワード検証部 94 はパスワード照合部 100、アクセスモード設定部 102 を備える。またコマンド処理部 92 にはパスワード書替部 98 が設けられている。

【0091】

このようなドライブ側の構成は、例えばハードディスクドライブを対象とした図 3 の実施形態と基本的に同じであるが、更にリムーバブル媒体として MO 媒体 172 を備えた MO カートリッジ 170 を使用する光ディスクドライブ 90 においては、パスワード検証部 94 に新たに有効期限管理部 104 を設けている。

有効期限管理部 104 は、デフォルト入力パスワード 60 が有効に使用される期限を管理しており、MO 媒体 172 もしくは光ディスクドライブ 90 に予め設定した有効期限が切れると、デフォルト入力パスワード 60 を異なる値に強制的に書き替え。

【0092】

このため、有効期間にあってはデフォルト入力パスワード 60 が書込読出パスワード 62 と同じであっても、有効期限が切れると書込読出パスワード 62 とは別の例えば 16 進値「3F231200」との EX-OR をとった値に変わってしまうため、パスワードの入力を行わない光ディスクドライブ 90 のアクセスは禁止されることになる。

【0093】

また逆に一定期間経過した時に、デフォルト入力パスワード 60 を、ある規則で書替えるように実装し、この規則で書替えを行ったときに、アクセス保護パスワードである例えば書込読出パスワード 62 と等しくなるような値を書替値として設定しておく。こうすれば一定期間経過した時に、パスワードを入力しなくともアクセスできるような使い方ができる。

【0094】

図 18 は、図 17 の光ディスクドライブ 90 におけるユーザのパスワード入力を必要としないアクセス保護の処理動作である。媒体メーカから出荷された時点で MO ディスク 172 は初期化处理されており、デフォルト入力パスワード 60、書込読出パスワード 62 及び読出オンリーパスワード 64 は、MO カートリッ

ジ 170 を初期化した際の初期値である 16 進の「CF23CF23h」が格納されている。

【0095】

このため、初期化されたパスワードの保存状態で光ディスクドライブの使用を開始すると、まずデフォルト入力パスワード 60 が読み出され、書込み処理 184 によってユーザ入力パスワード 66 としてユーザ入力パスワード格納領域 202 に書き込まれる。

続いてデフォルト入力パスワード 60 の書込みを受けたユーザ入力パスワード 66 と書込読出パスワード 62 の照合比較処理 186 を行い、照合一致が得られることでアクセス許可 188、即ち書込読出モードの設定が行われる。このため、図 17 の光ディスクドライブ 90 にあっても、ユーザはパスワード入力が必要とすることなく、MO カートリッジ 170 のアクセス許可状態を確立することができる。

【0096】

図 19 は、図 18 のようなデフォルト入力パスワードに基づくアクセス許可が確立された書込読出モードの状態で、パスワード書替えを行った場合である。このパスワード書替えにあっては、図 18 のデフォルト入力パスワード 60 の初期値「CF23CF23h」をパスワード書替コマンド 190 に基づく書替処理 192 によって別の値「AB89AB89h」に書き替えている。

【0097】

このようにデフォルト入力パスワード 60 を別の値に書き替えてしまうと、次に光ディスクドライブ 90 の使用を開始したときユーザがパスワードを入力しないと、まず書込処理 194 によってユーザ入力パスワード 66 が変更後のデフォルト入力パスワード 60 の値「AB89AB89h」に書き替えられ、次に書込読出パスワード 62 の値「CF23CF23h」との照合比較処理 196 が行われ、この場合は照合不一致となってアクセス禁止 198、即ちセキュリティモードが設定されてしまう。

【0098】

この図 19 のようなデフォルト入力パスワード 60 の書替えは、次のような場

合に有効である。まず光ディスクドライブ 90 の本来の使用者 A 氏は、図 18 のようにデフォルト入力パスワード 60 及び書込読出パスワード 62 を同じ初期値「CF23CF23h」とした状態で秘書の B 氏に処理を依頼する。依頼を受けた B 氏は、パスワードを知らなくとも電源を投入することでデフォルト入力パスワード 60 に基づくアクセス許可による読出書込モードが確立され、光ディスクドライブ 90 を使用した処理を行うことができる。

【0099】

ここで本来の使用者である A 氏は仕事を依頼した B 氏に対し、仕事を終了したならばパスワード書替コマンド「Change Default Psw "AB89AB89"」を入力するように依頼しておく。そこで、依頼を受けた B 氏は、業務が終了したならば A 氏から指示されたコマンドを入力する。

このコマンドを入力すると、図 19 のように、デフォルト入力パスワード 60 は「AB89AB89h」に書き替えられてしまう。

【0100】

このため本来の使用者 A 氏より依頼を受けて業務を行った B 氏が、業務を終了してデフォルト入力パスワード 60 を書き替えて MO カートリッジ 170 のイジェクト操作を行うと、このイジェクト操作に伴う指示を受けて、ワークメモリ 160 に展開しているデフォルト入力パスワード 60、書込読出パスワード 62 及び読出オンリーパスワード 64 は、MO カートリッジ 170 のパスワード格納領域 182 にライトバックされた後に MO カートリッジ 170 が排出される。

【0101】

このため、MO カートリッジ 170 が排出された後は、再度、MO カートリッジ 170 を光ディスクドライブ 90 に挿入しても、このときワークメモリ 106 に読み出されるデフォルト入力パスワード 60 は、図 19 のように書込読出パスワード 62 とは異なった値に変更されており、書込読出パスワード 60 の値をパスワードとして入力しない限り、MO カートリッジ 170 のアクセスは一切禁止することができる。

【0102】

即ち本来の使用者 A 氏は、B 氏に業務が終了したらデフォルト入力パスワード

書替コマンドの入力を指示しておくことで、B氏が作業を終了した後に、第3者は勿論のことB氏がA氏の光ディスクドライブ90を使用するために電源を投入しても、本来の使用者であるA氏しか分かっていないパスワード「CF23CF23h」を入力しない限り、光ディスクドライブ90はセキュリティモードとなってアクセスを一切禁止することができる。

【0103】

図20は、図7の保存形態1に対応した光ディスクドライブ90の実施形態であり、この実施形態にあつては、デフォルト入力パスワード、書込読出パスワード及び読出オンリーパスワードをドライブ本体側に保存したことを特徴とする。

図20において、光ディスクドライブ90の不揮発性メモリ108にはパスワード格納領域200が設けられ、ここにデフォルト入力パスワード60、書込読出パスワード62及び読出オンリーパスワード64を格納している。またワークメモリ106にはユーザ入力パスワード格納領域202が設けられ、ここにユーザ入力パスワード66を格納している。

【0104】

デフォルト入力パスワードを用いたアクセス保護のため光ディスクドライブ90には、コマンド処理部92、パスワード検証部94及びアクセス実行部96が設けられる。パスワード検証部94はパスワード照合部100、アクセスモード設定部102を備える。またコマンド処理部92にはパスワード書替部98が設けられている。更にパスワード検証部94に新たに有効期限管理部104を設けている。

【0105】

図21は、図7の保存形態3に対応した光ディスクドライブ90の実施形態であり、この実施形態にあつては光ディスクドライブ90の不揮発性メモリ108のパスワード格納領域200にデフォルト入力パスワード60を保存し、一方、書込読出パスワード62及び読出オンリーパスワード64についてはリムーバブル媒体であるMOカートリッジ170のパスワード格納領域182に保存したことを特徴とする。

【0106】

このため、MOカートリッジ170を光ディスクドライブ90に挿入した場合には、パスワード検証部94はアクセス実行部96を介して、まずMOカートリッジ170のパスワード格納領域182から書込読出パスワード62と読出オンリーパスワード64を読み出してワークメモリ106に展開する。

図22は、図7の保存形態4を適用した光ディスクドライブ90の実施形態であり、保存形態4にあっては光ディスクドライブ90の不揮発性メモリ108のパスワード格納領域200にアクセス保護用の書込読出パスワード62及び読出オンリーパスワード64を保存し、一方、デフォルト入力パスワード60はMOカートリッジ170のパスワード格納領域182に保存している。

【0107】

このため、MOカートリッジ170を光ディスクドライブ90に挿入した場合には、パスワード検証部94はアクセス実行部96を介してMOカートリッジ170からデフォルト入力パスワード60を読み出し、ワークメモリ160のパスワード格納領域204に図示のように展開する。

図23は、光ディスクドライブ90におけるユーザがパスワードを入力しなかった場合のアクセス保護処理のフローチャートであり、図17の保存形態2の場合を例にとって説明すると次のようになる。

【0108】

光ディスクドライブ90にMOカートリッジ170を挿入すると、ステップS1でデフォルト入力パスワード60を読み出してユーザ入力パスワード領域にユーザ入力パスワード66として書込み設定する。続いてステップS2で、ユーザ入力パスワード66と書込読出パスワード62を比較照合し、ステップS3で照合一致が得られると、ステップS6の書込読出モードを設定する。

【0109】

照合不一致であれば、ステップS4でユーザ入力パスワード66と読出オンリーパスワード64を比較照合し、ステップS5で照合一致が得られれば、ステップS7で読出オンリーモードを設定する。照合不一致であれば、ステップS8でセキュリティモードとし、パスワードを伴わないアクセスは一切禁止とする。このステップS6、S7で書込読出モードあるいは読出モードが設定されると、ス

ステップ S 9 でパスワード検証部 9 4 に設けた有効期限管理部 1 0 4 による期限管理処理が行われる。

【0110】

図 2 4 は、図 2 3 のステップ S 9 の期限管理処理の一実施形態のフローチャートである。この期限管理処理にあつては、まずステップ S 1 でデフォルト入力パスワードの初期化あるいはコマンドによる変更の有無をチェックし、初期化または変更があれば、ステップ S 2 でカウンタ D P C を $D P C = 0$ にセットし、ステップ S 3 でカウンタ D P C を 1 つインクリメントする。

【0111】

もちろん、デフォルト入力パスワードの初期化あるいは変更がなければ、ステップ S 2 をスキップして、ステップ S 3 でカウンタ D P C を 1 つインクリメントする。続いてステップ S 4 で、カウンタ D P C は予め定めた有効期限を与える規定値 N X X 以上か否かチェックする。

カウンタ D P C の値が規定値 N X X 未満であればステップ S 5 をスキップするが、カウンタ D P C が規定値 N X X 以上となった場合はステップ S 5 に進み、光ディスクドライブ 9 0 内で乱数列 R X を発生し、デフォルト入力パスワードの値 P D と乱数列 R X との排他論理和を求め、これを新たなデフォルト入力パスワードの値とする。

【0112】

即ち、この実施形態にあつては、カウンタ D P C によって光ディスクドライブ 9 0 の使用回数を計数しており、使用回数が規定値 N X X に達すると、乱数列を使用して強制的にデフォルト入力パスワードをユーザの知り得ない値に変更し、有効期限以降のパスワードを入力しないアクセス許可を禁止する。

図 2 5 は、図 2 のデフォルト入力パスワードの期限管理処理の他の実施形態のフローチャートである。この期限管理処理にあつては、ステップ S 1 でデフォルト入力パスワードの初期化あるいは変更の有無をチェックしており、初期化または変更があれば、ステップ S 2 でカウンタ D P C に所定の有効期限の時刻をセットする。続いてステップ S 3 で、現在時刻がカウンタ D P C にセットした有効期限の時刻以降か否かチェックする。

【0113】

現在時刻がカウンタDPCの有効期限の時刻以降であった場合には、ステップS5に進み、図23の場合と同様、光ディスクドライブ90内で乱数列RXを発生して、そのときのデフォルト入力パスワードの値DPとの排他論理和で置き換え、デフォルト入力パスワードの値を異なる値に強制的に変更し、有効期限以降でのパスワードの入力によらない光ディスクドライブ90のアクセスを一切禁止する。

【0114】

また現在時刻がカウンタDPCの有効期限の時刻以降となってステップS5に進んだ場合、デフォルト入力パスワード60をアクセス保護パスワード例えば書込読出パスワード62と等しい値に変更することで、一定期間経過した時に、パスワードを入力しなくともアクセスできるような使い方が設定できる。

ここで光ディスクドライブ90にあっては、図23のフローチャートでユーザがパスワードを入力した場合の処理を例にとっているが、ユーザがパスワードを入力した場合の処理については、ハードディスクドライブにおける図13のフローチャートと同じである。またユーザに必ずパスワード入力操作の実行を行わせるハードディスクドライブの図14のフローチャートの処理についても、そのまま光ディスクドライブ90に適用することができる。

【0115】

尚、上記の実施形態は、記憶装置としてハードディスクドライブ、光ディスクドライブを例にとるものであったが、これ以外に磁気テープドライブ、フロッピーディスクドライブを含むことはもちろんである。また本発明は記憶装置に限定されず、パスワードによるアクセス保護を行う装置やシステム一般につきそのまま適用することができる。

【0116】

【発明の効果】

以上説明してきたように本発明によれば、パスワードを用いて保護する装置側例えば記憶装置側にデフォルト入力パスワードを格納し、ユーザからのパスワード

ド入力がない場合にはデフォルト入力パスワードをユーザ入力パスワードとみなしてパスワードの検証を行うため、デフォルト入力パスワードとアクセス保護用パスワードを同じ値にしておくことによって、ユーザがパスワード入力を行わなくともアクセス保護を解除して通常コマンドによるアクセスができ、ユーザによるパスワード入力を大幅に省略することができる。

【0117】

また記憶装置において既にアクセスが許可されている場合には、デフォルト入力パスワードのユーザによる書替えを可能とすることで、ユーザは必要に応じてパスワード入力を必要としないアクセス保護とパスワード入力を必要とするアクセス保護を使い分けることができる。

更にデフォルト入力パスワードの有効期限を管理し、期限を過ぎた場合にはデフォルト入力パスワードをユーザが知り得ない別な値に強制的に変更してしまうことで、パスワードの入力を省略した記憶装置のアクセス可能な状態を一定期間だけ限定的に継続させることができ、パスワード入力を省略できるという無防備な状態が長期間に亘って継続することを未然に防止できる。

【図面の簡単な説明】

【図1】

本発明の原理説明図

【図2】

本発明が適用されるハードディスクドライブのブロック図

【図3】

パスワードをドライブ本体に保存した本発明の実施形態の機能ブロック図

【図4】

ユーザのパスワード入力がない場合のデフォルト入力パスワードでアクセス許可を獲得するアクセス保護処理の説明図

【図5】

デフォルト入力パスワード及びアクセス制御用パスワードのコマンド書替処理の説明図

【図 6】

本発明におけるアクセス種別の説明図

【図 7】

本発明におけるパスワードの保存形態の説明図

【図 8】

パスワードを媒体のみに保存した本発明の実施形態の機能ブロック図

【図 9】

図 8 の媒体内のパスワード保存領域の説明図

【図 10】

パスワードをドライブ本体と媒体に分けて保存した本発明の実施形態の機能ブロック図

【図 11】

パスワードをドライブ本体と媒体に分けて保存した本発明の他の実施形態の機能ブロック図

【図 12】

ユーザのパスワード入力がない場合のアクセス保護処理のフローチャート

【図 13】

ユーザがパスワードを入力した場合のアクセス保護処理のフローチャート

【図 14】

ユーザがパスワード入力操作を必ず必要とするアクセス保護処理のフローチャート

【図 15】

本発明が適用される光ディスクドライブのブロック図

【図 16】

MOカートリッジをローディングした装置内部構造の説明図

【図 17】

パスワードをリムーバブル媒体のみに保存した本発明の実施形態の機能ブロック図

【図 18】

MOドライブに対しユーザのパスワード入力がなくデフォルト入力パスワードでアクセス許可を獲得するアクセス保護処理の説明図

【図19】

デフォルト入力パスワードによるアクセスを禁止するためのパスワード書替処理の説明図

【図20】

パスワードをMOドライブ本体に保存した本発明の実施形態の機能ブロック図

【図21】

パスワードをMOドライブ本体とリムーバブル媒体に分けて保存した本発明の実施形態の機能ブロック図

【図22】

パスワードをMOドライブ本体とリムーバブル媒体に分けて保存した本発明の他の実施形態の機能ブロック図

【図23】

MOドライブにおけるユーザのパスワード入力がない場合のアクセス保護処理のフローチャート

【図24】

カウンタで使用回数を計数してデフォルト入力パスワードの期限を管理する図22の有効期限管理処理のフローチャート

【図25】

デフォルト入力パスワードの期限となる時刻を設定して管理する図22の有効期限管理処理のフローチャート

【符号の説明】

10, 111 : エンクロージャ

12, 110 : コントロールボード

22, 112 : メインコントロールユニット (MCU)

38, 106 : ワークメモリ (RAM)

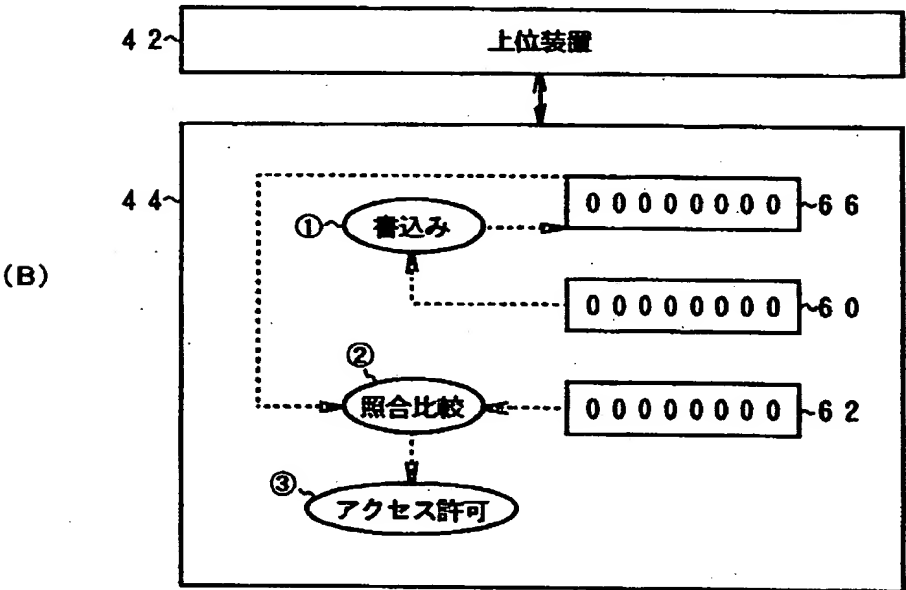
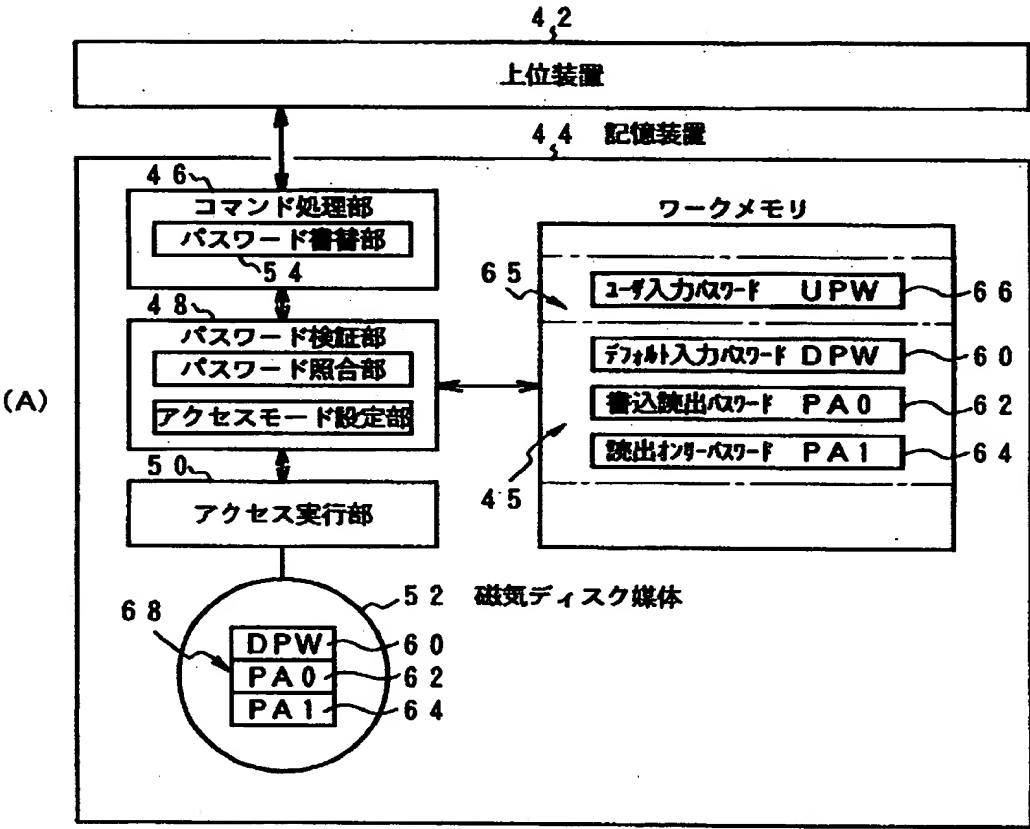
40, 108 : 不揮発性メモリ (フラッシュROM)

- 42 : 上位装置
- 44 : ハードディスクドライブ (HDD)
- 46, 92 : コマンド処理部
- 48, 94 : パスワード検証部
- 50, 96 : アクセス実行部
- 52 : 磁気ディスク媒体
- 54, 98 : パスワード書替部
- 56, 100 : パスワード照合部
- 58, 102 : アクセスモード設定部
- 60 : デフォルト入力パスワード (DPW)
- 62 : 書込読出パスワード (アクセス保護用パスワード)
- 64 : 書込オンリーパスワード (アクセス保護用パスワード)
- 65 : ユーザ入力パスワード領域
- 66 : ユーザ入力パスワード (UPW)
- 67 : パスワード格納領域
- 68 : パスワード保存領域
- 70 : ディスク管理領域
- 90 : 光ディスクドライブ (ODD)
- 102 : 有効期限管理部
- 170 : MOカートリッジ (光磁気ディスクカートリッジ)
- 172 : MO媒体 (光磁気ディスク媒体)

【書類名】 図面

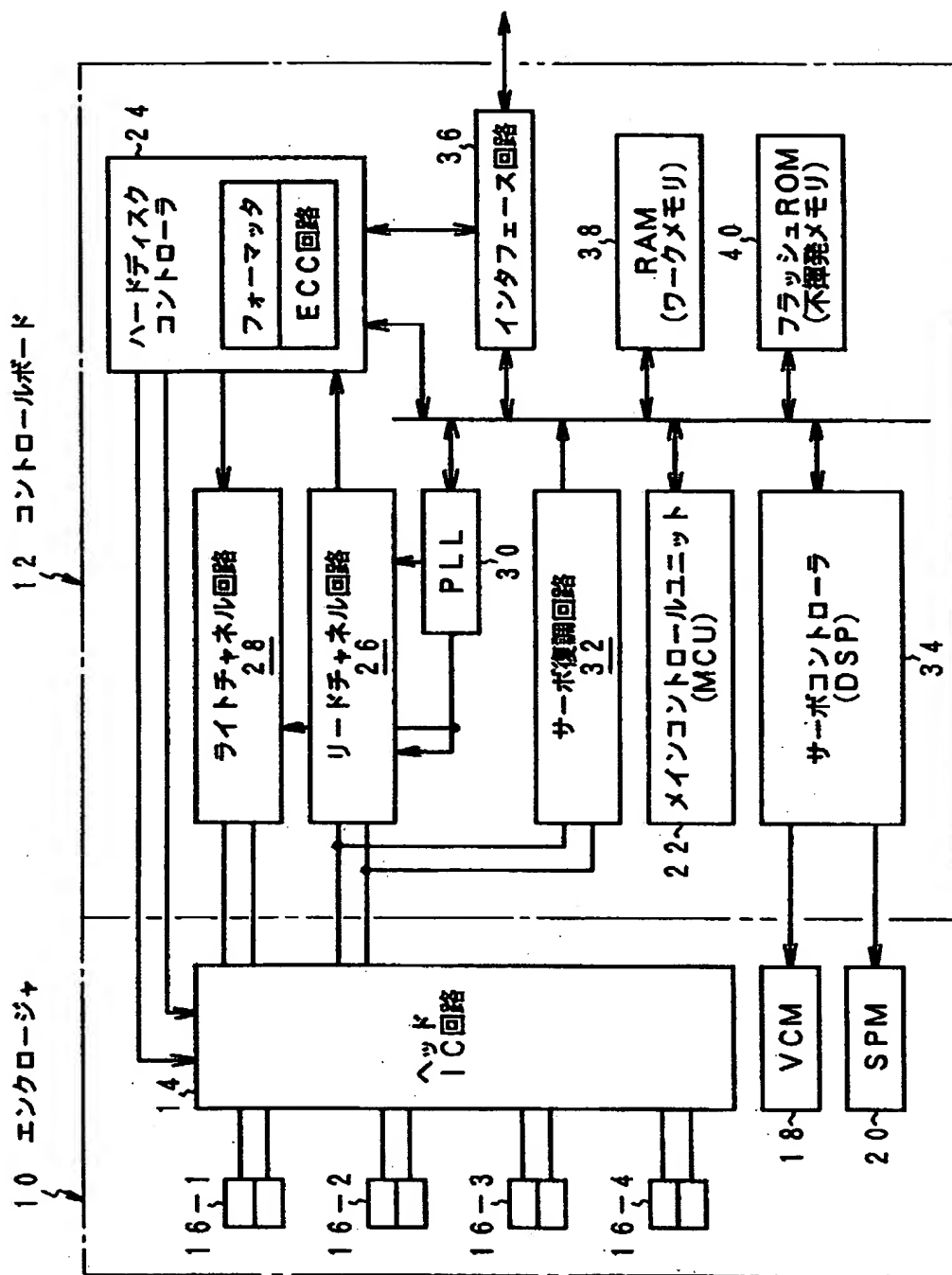
【図 1】

本発明の原理説明図



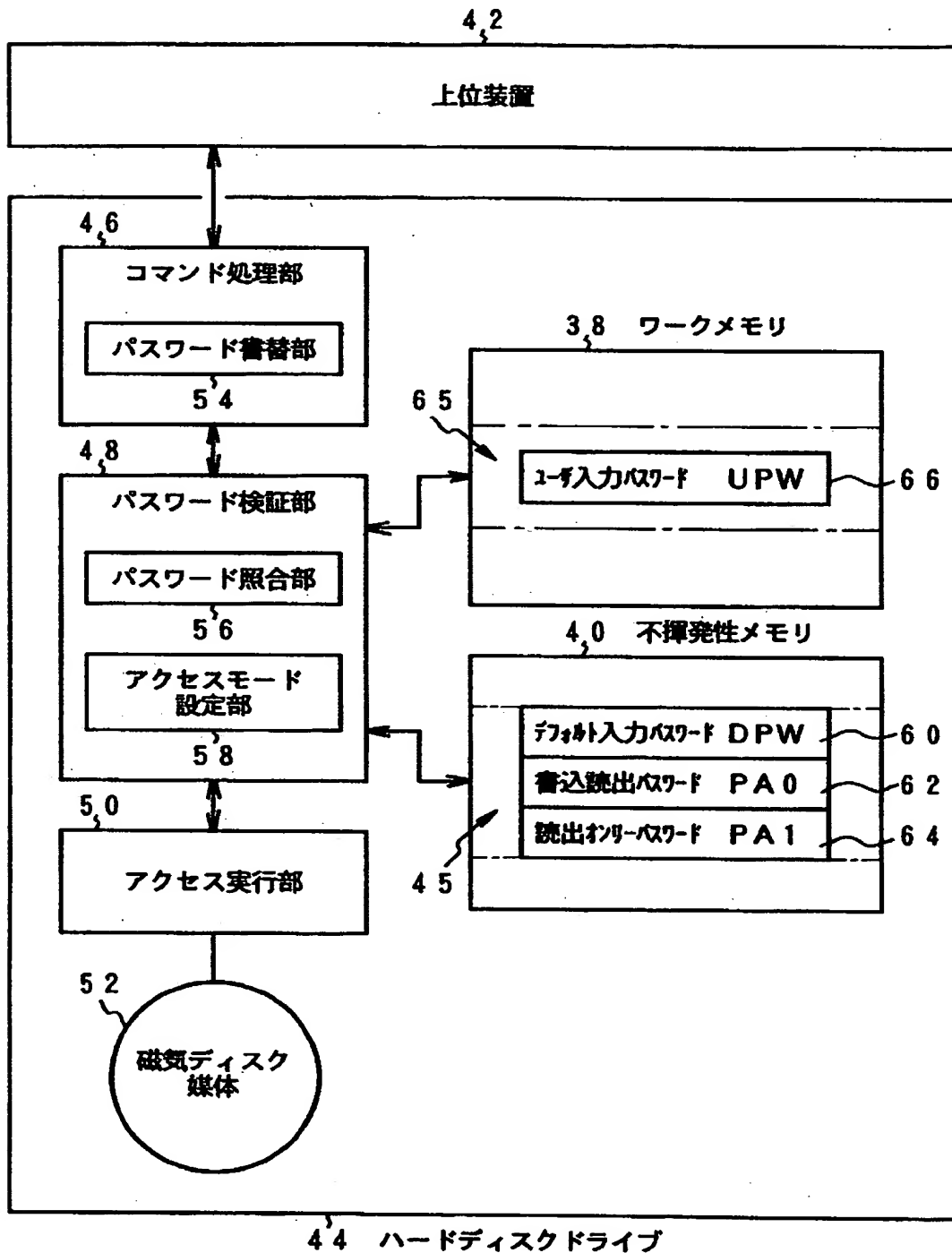
【図 2】

本発明が適用されるハードディスクドライブのブロック図



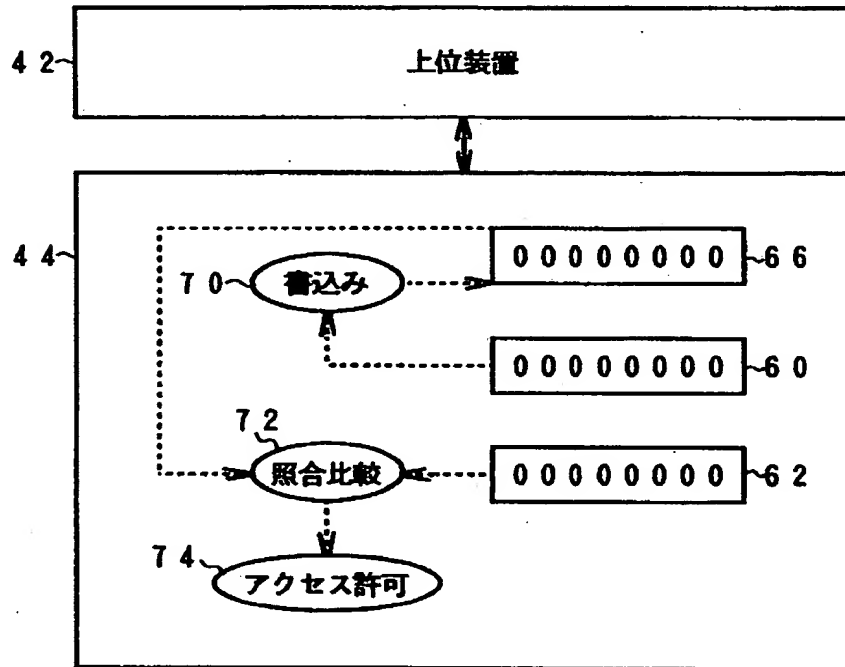
【図3】

パスワードをドライブ本体に保存した本発明の実施形態の機能ブロック図



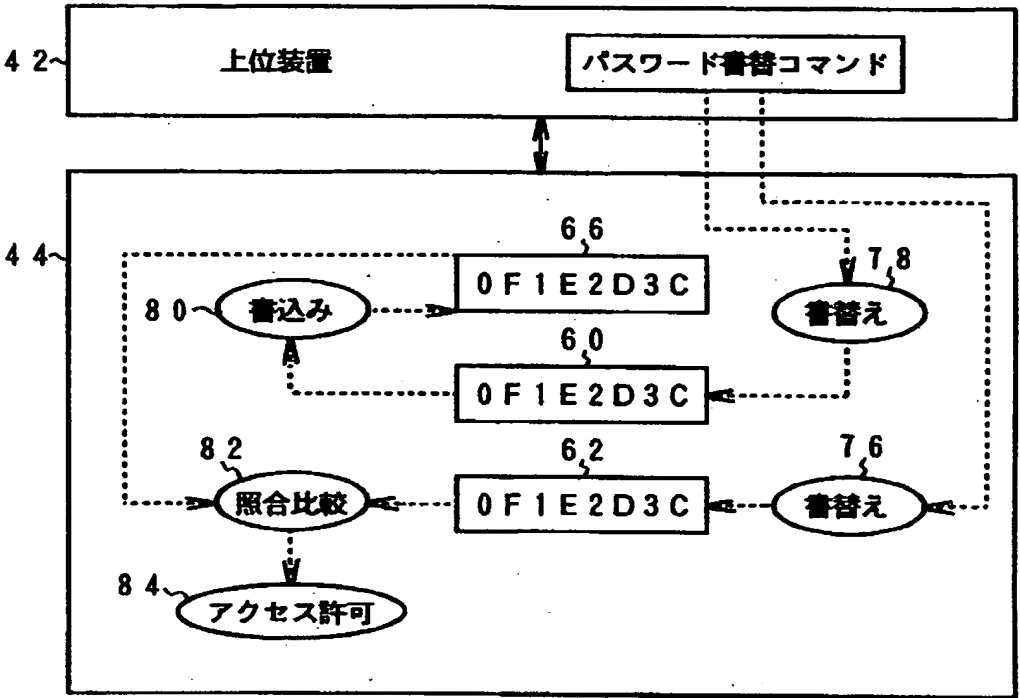
【図 4】

ユーザのパスワード入力がない場合のデフォルト入力パスワードでアクセス許可
を獲得するアクセス保護処理の説明図



【図 5】

デフォルト入力パスワード及びアクセス制御用パスワードのコマンド書替処理の説明図



【図 6】

本発明におけるアクセス種別の説明図

モード	アクセス内容
書込読出モード	通常の読出コマンドと書込コマンドを受け付ける。 デフォルト入力、読出、及び読出書込の各パスワードの変更を許可する。
読出オンリーモード	通常の読出コマンドのみを受け付ける。 デフォルト入力、読出、及び読出書込の各パスワードの変更を許可する。
セキュリティモード	アクセス不可とする。 パスワード入力を伴う読出コマンド又は書込コマンドのみを受け付ける。

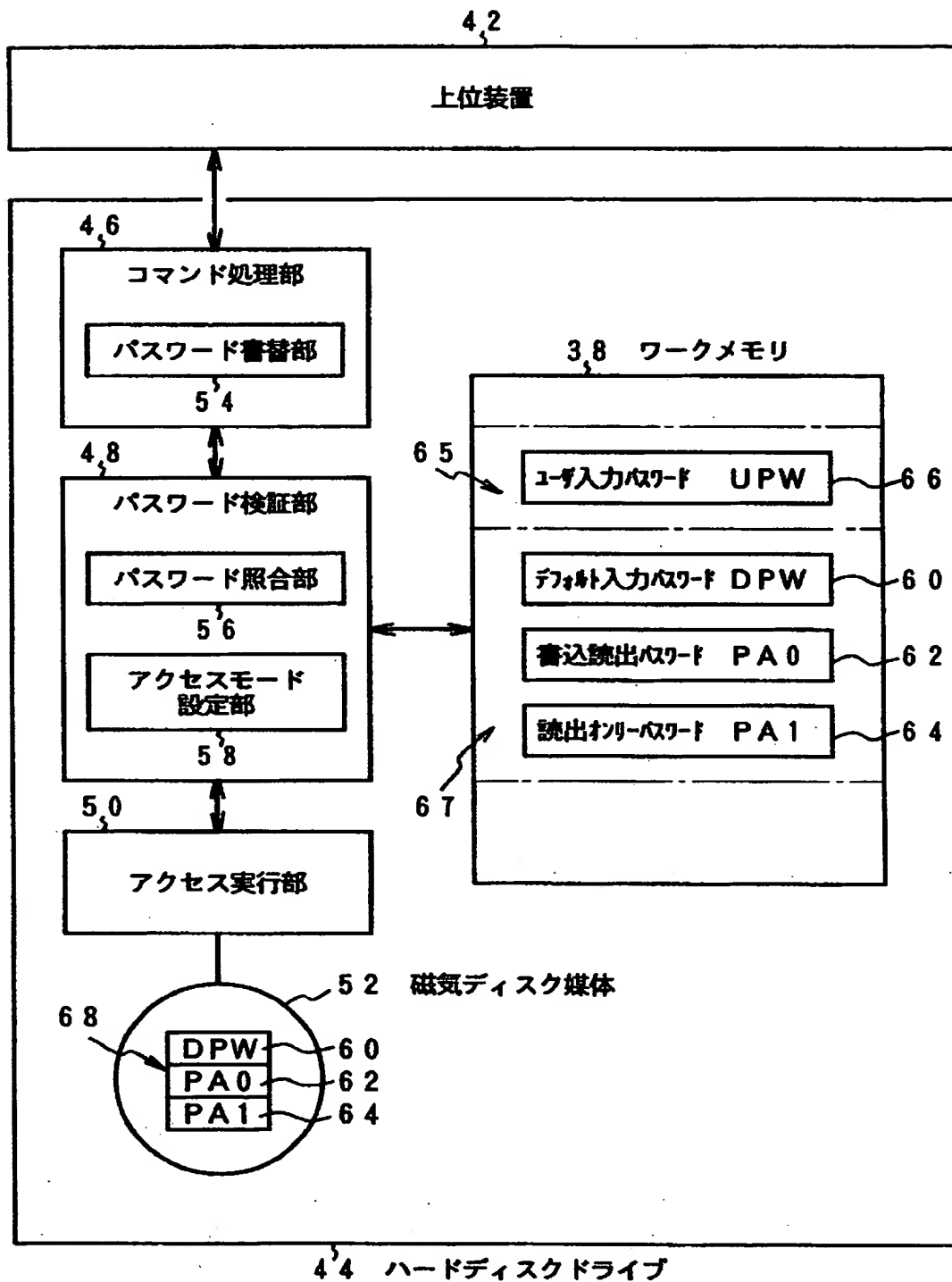
【図 7】

本発明におけるパスワードの保存形式の説明図

保存形態	デフォルト入力 パスワード格納位置	パスワード格納位置
1	ドライブ	ドライブ
2	媒体	媒体
3	ドライブ	媒体
4	媒体	ドライブ

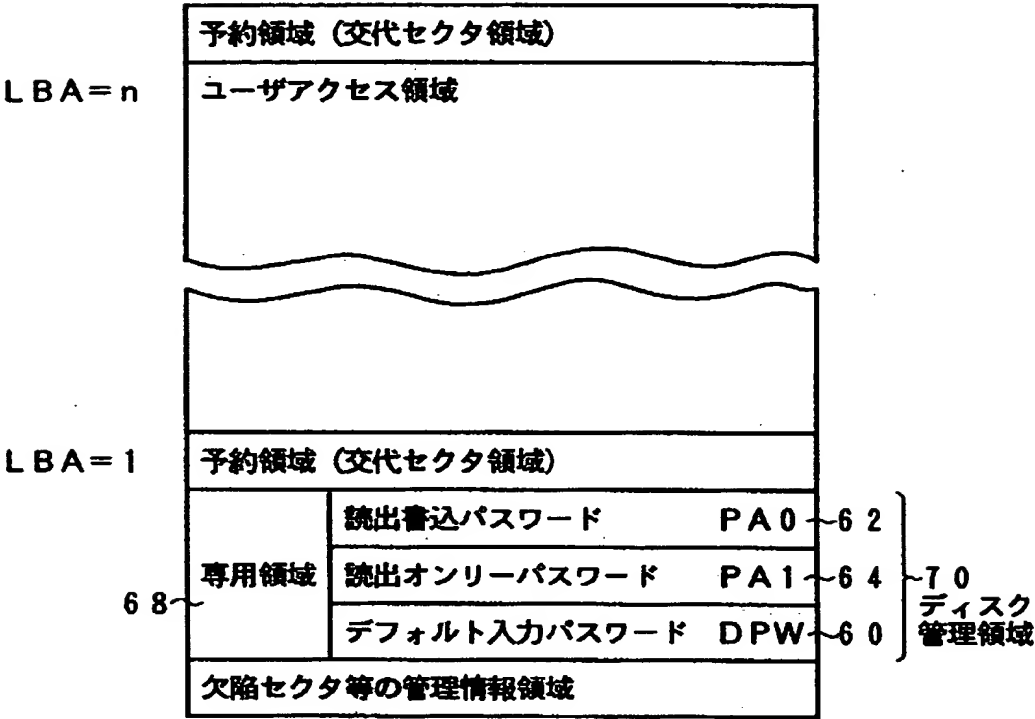
【図 8】

パスワードを媒体のみに保存した本発明の実施形態の機能ブロック図



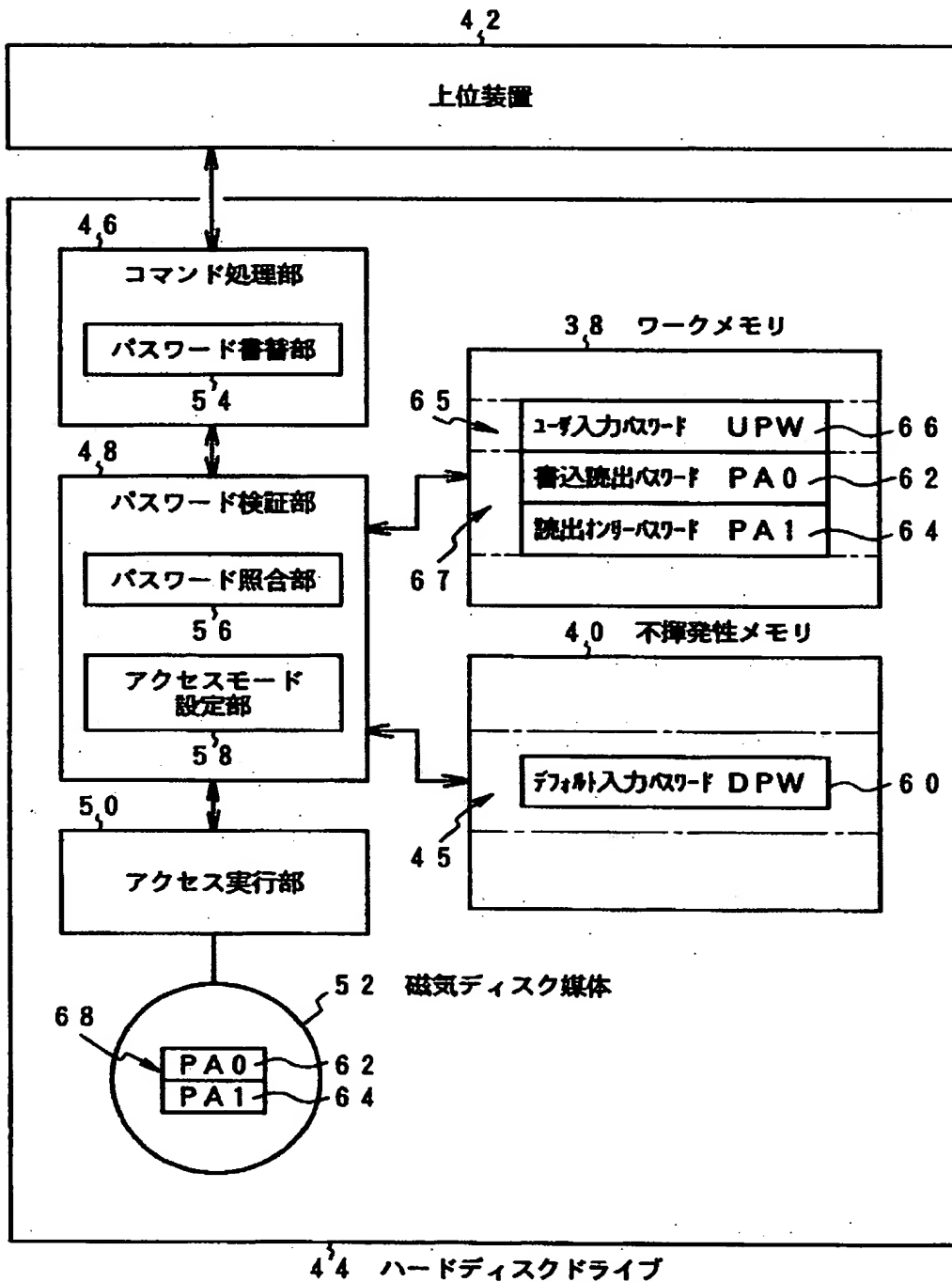
【図 9】

図 8 の媒体内のパスワード保存領域の説明図



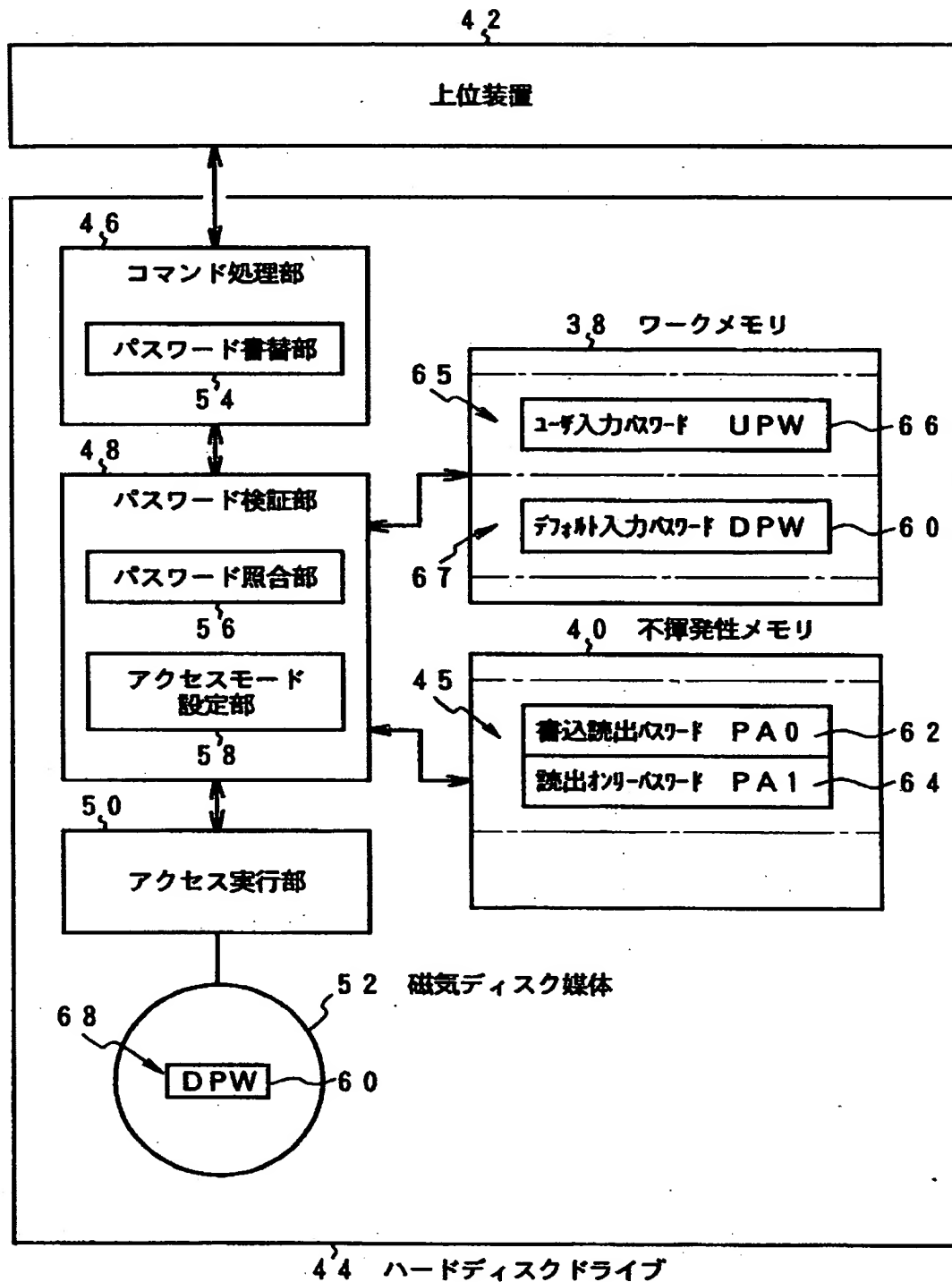
【図 10】

パスワードをドライブ本体と媒体に分けて保存した本発明の実施形態の機能ブロック図



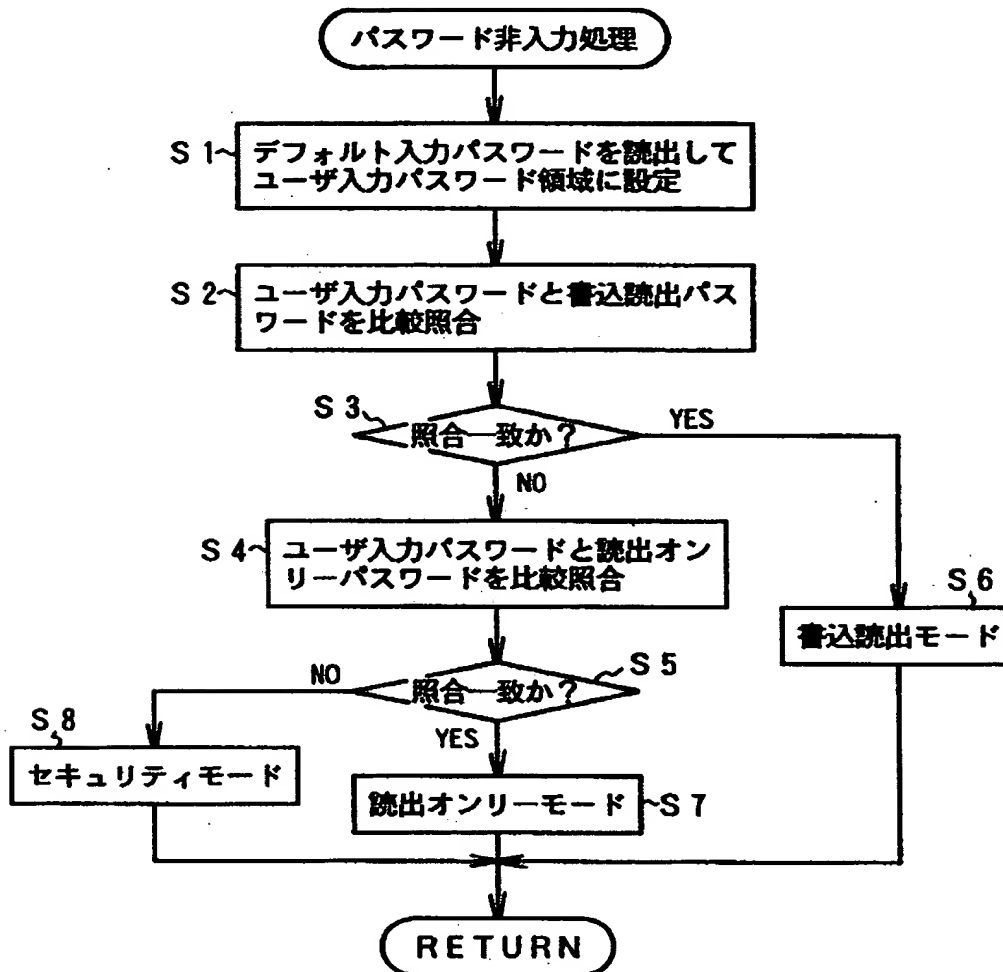
【図 11】

パスワードをドライブ本体と媒体に分けて保存した本発明の他の実施形態の
機能ブロック図



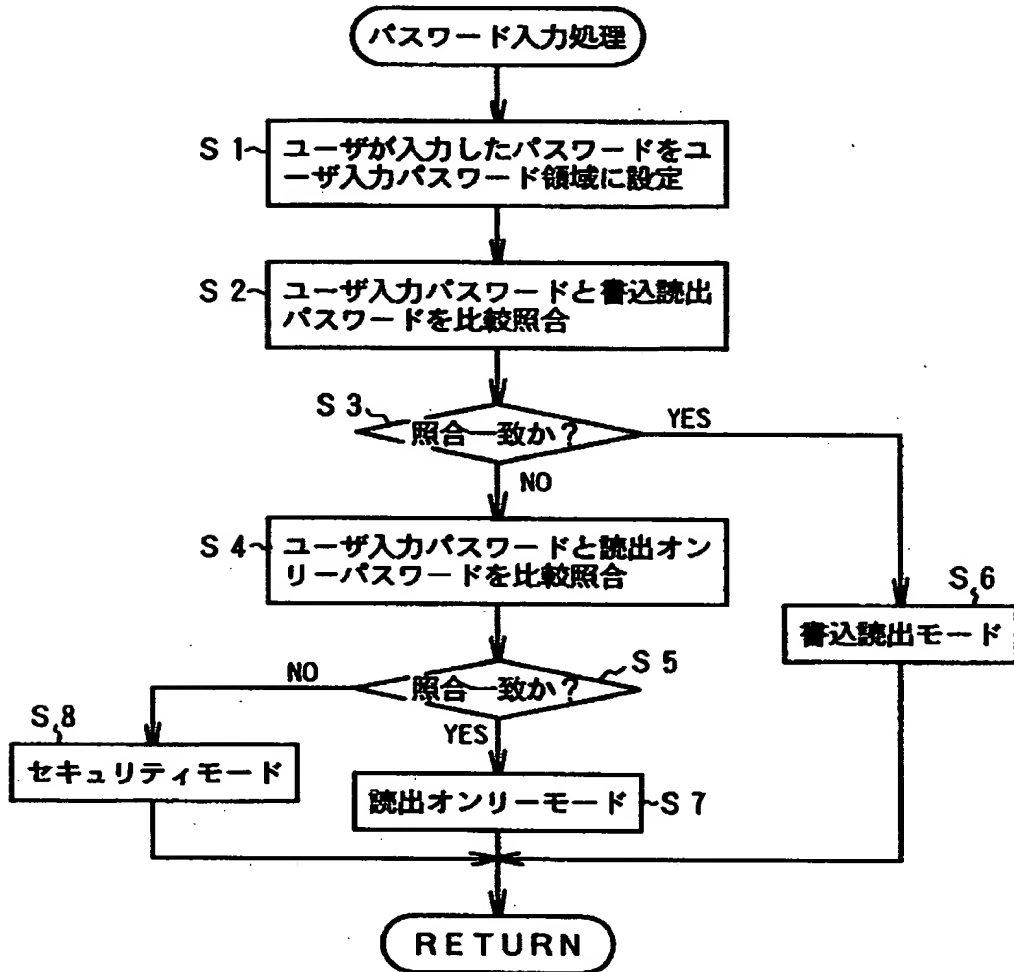
【図 12】

ユーザのパスワード入力がない場合のアクセス保護処理のフローチャート



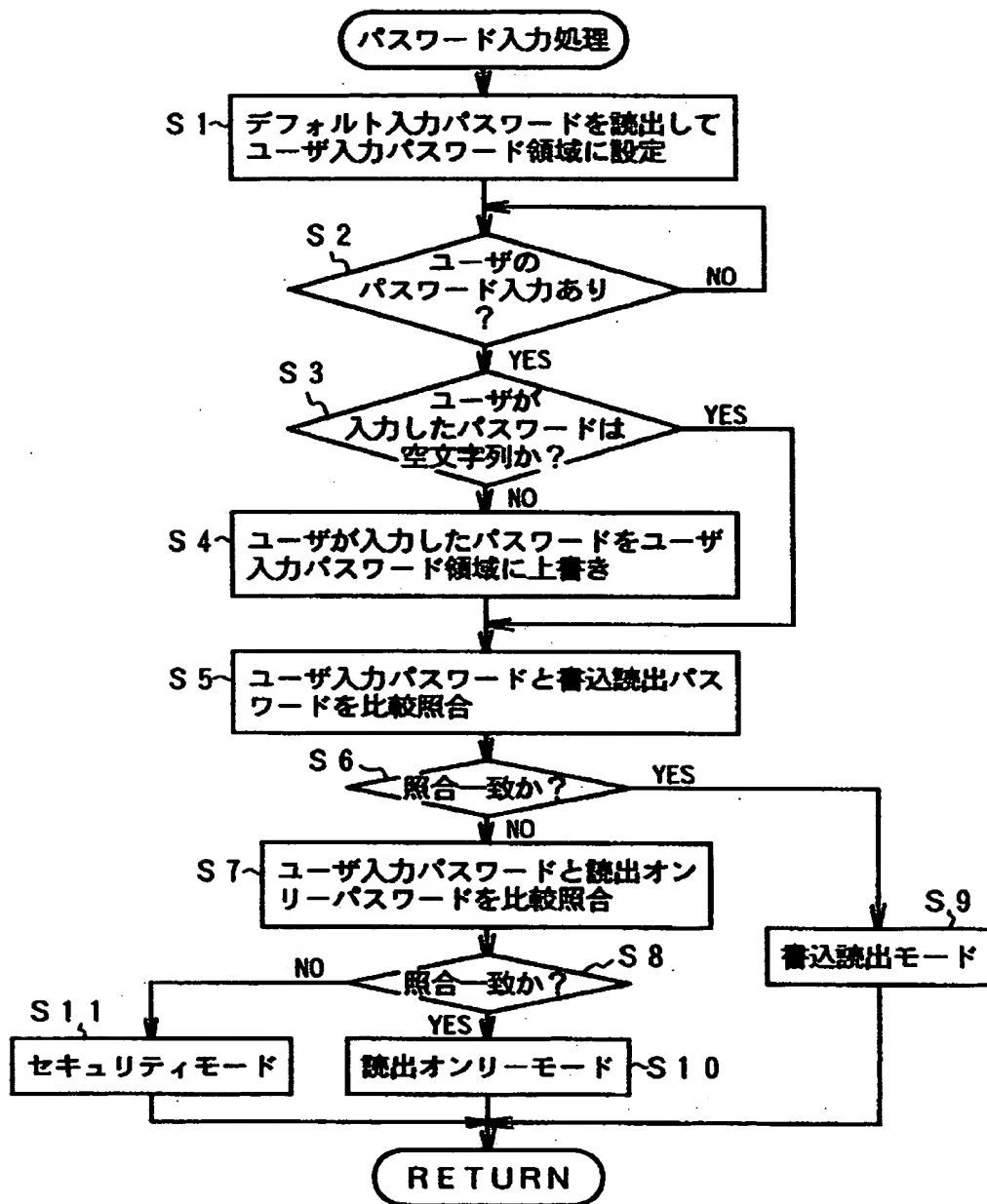
【図 13】

ユーザがパスワードを入力した場合のアクセス保護処理のフローチャート



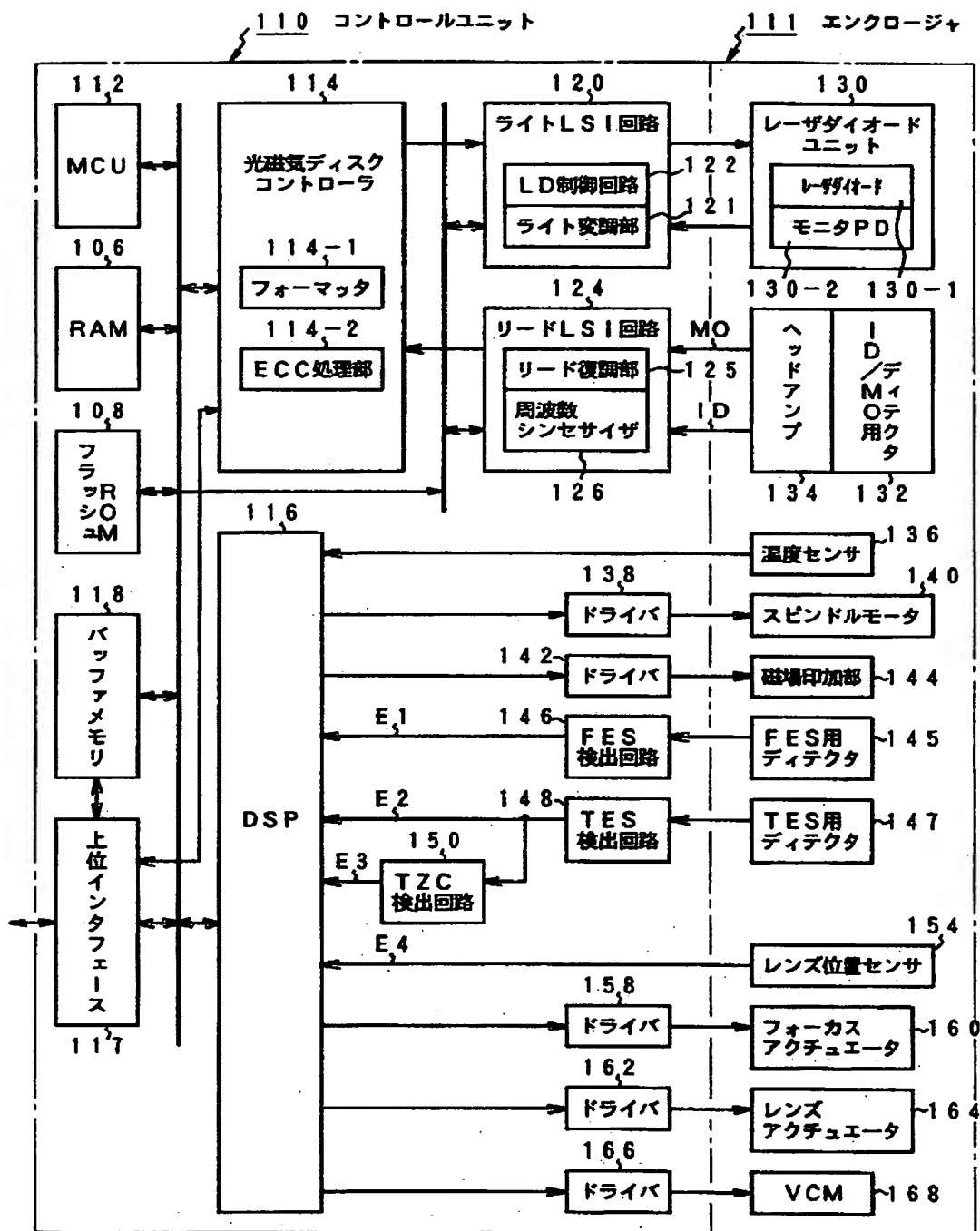
【図 14】

ユーザがパスワード入力操作を必ず必要とするアクセス保護処理のフローチャート



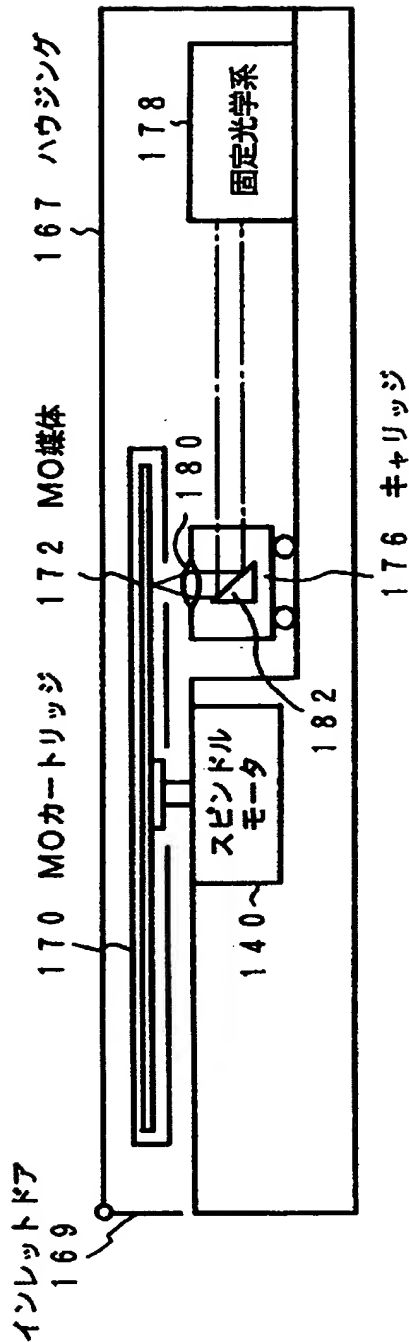
【図 15】

本発明が適用される光ディスクドライブのブロック図



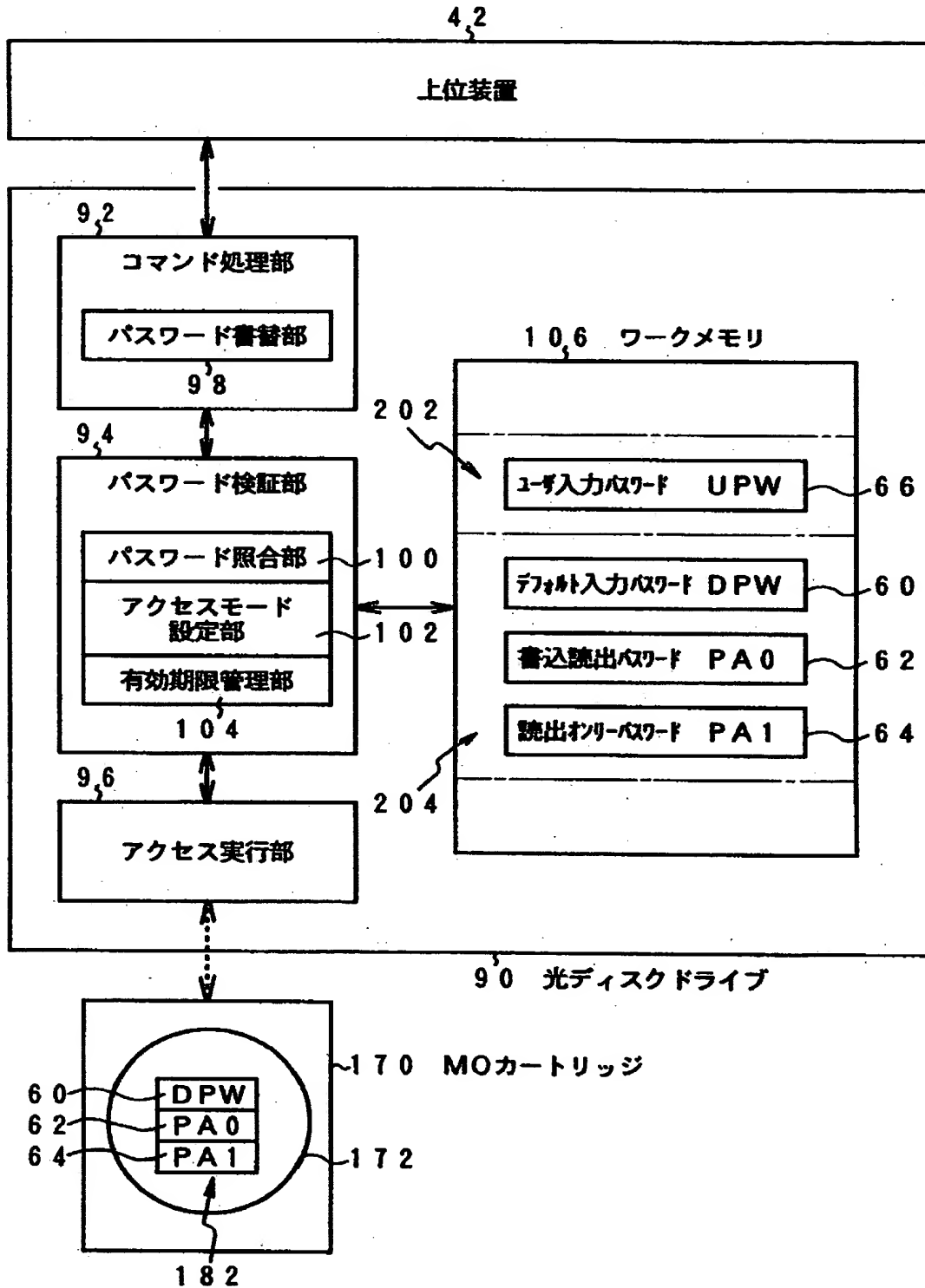
MOカートリッジをローディングした装置内部構造の説明図

【図 16】



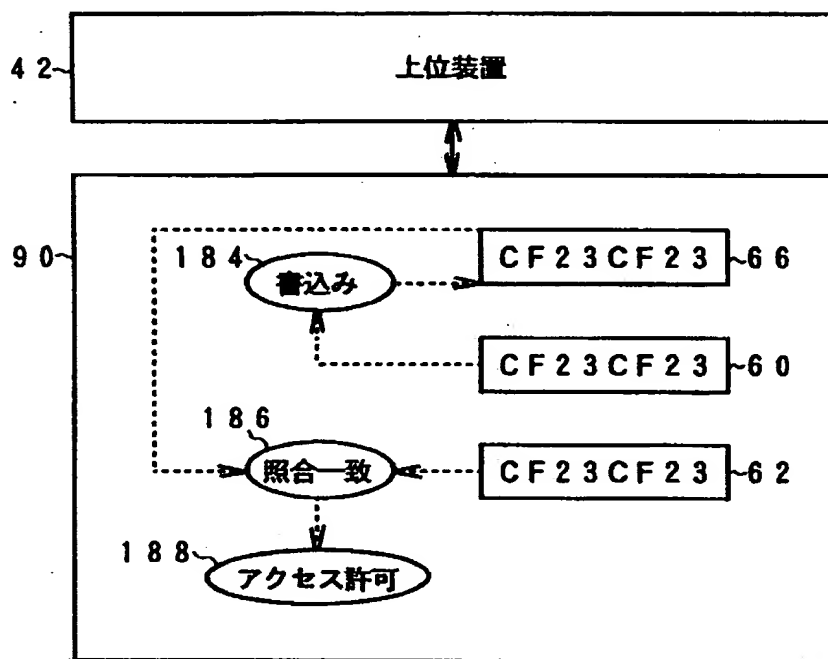
【図 17】

パスワードをリムーバブル媒体のみに保存した本発明の実施形態の機能ブロック図



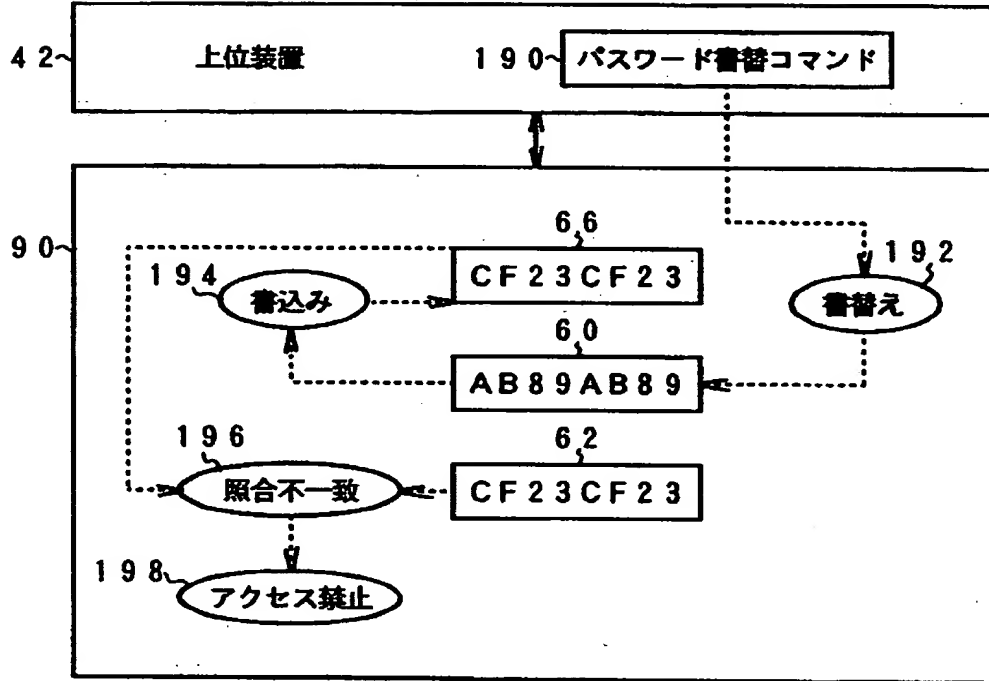
【図 18】

MOドライブに対しユーザのパスワード入力がなくデフォルト入力パスワードで
アクセス許可を獲得するアクセス保護処理の説明図



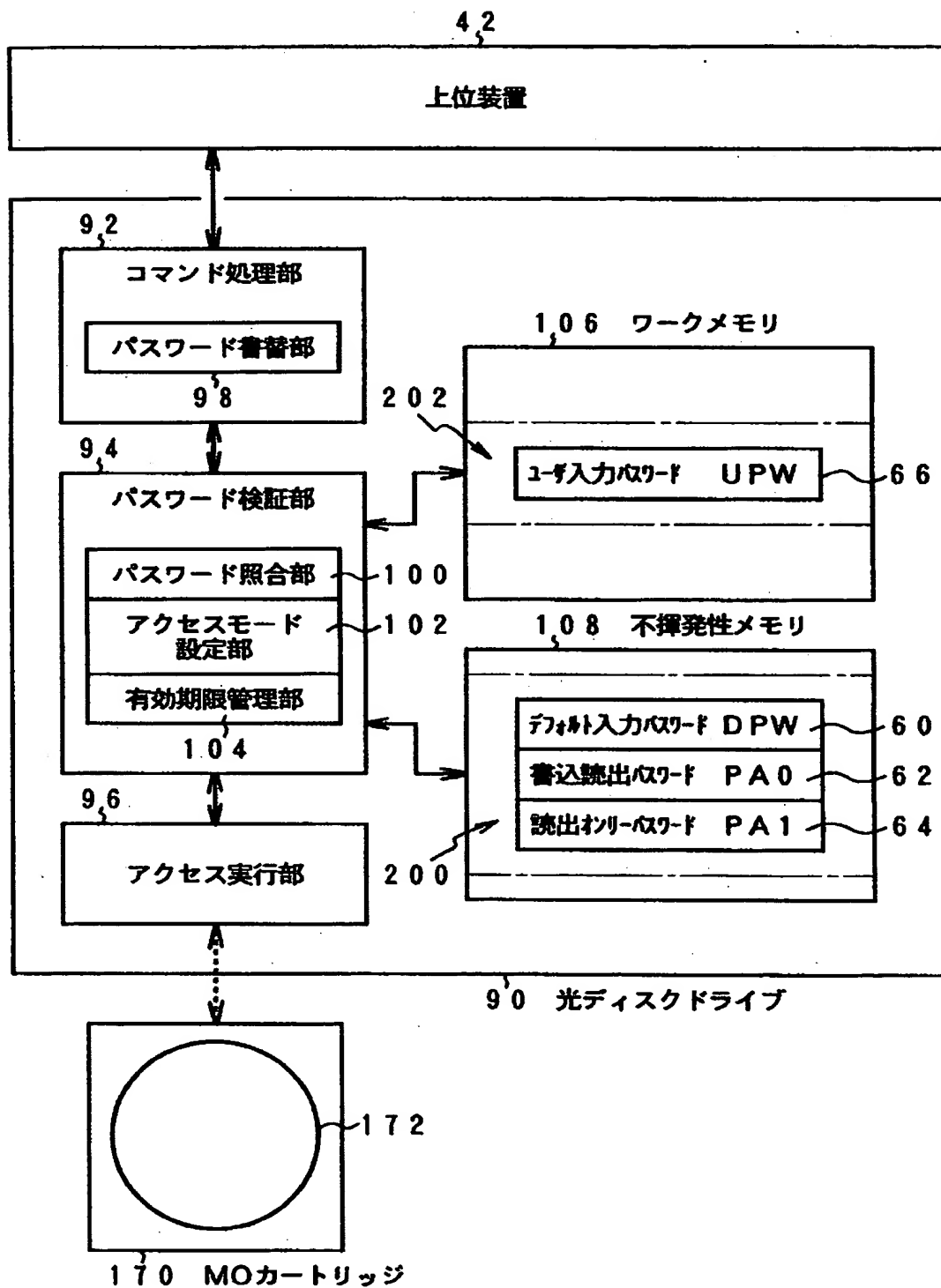
【図 19】

デフォルト入力パスワードによるアクセスを禁止するためのパスワード書替処理の説明図



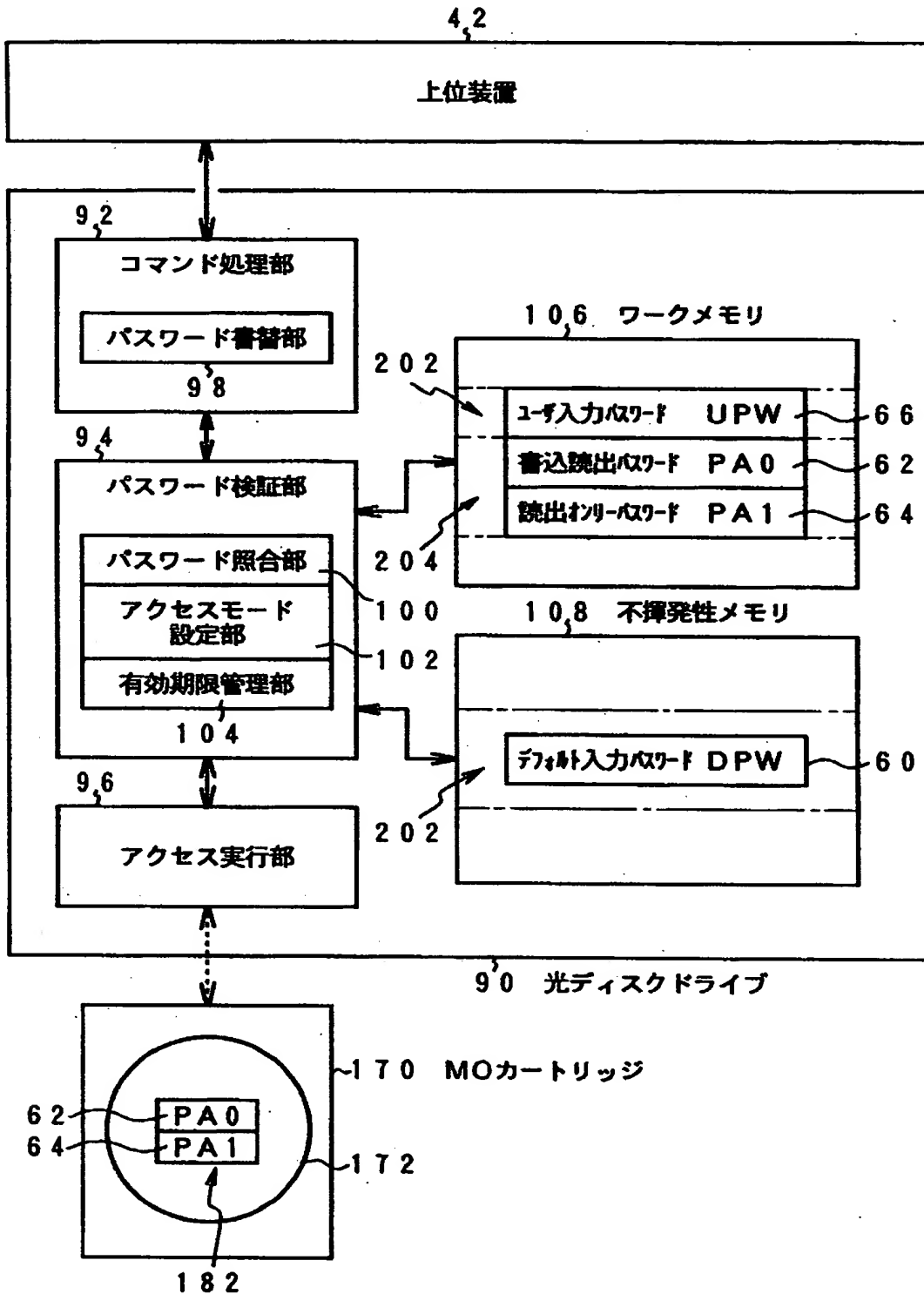
【図 20】

パスワードをMOドライブ本体に保存した本発明の実施形態の機能ブロック図



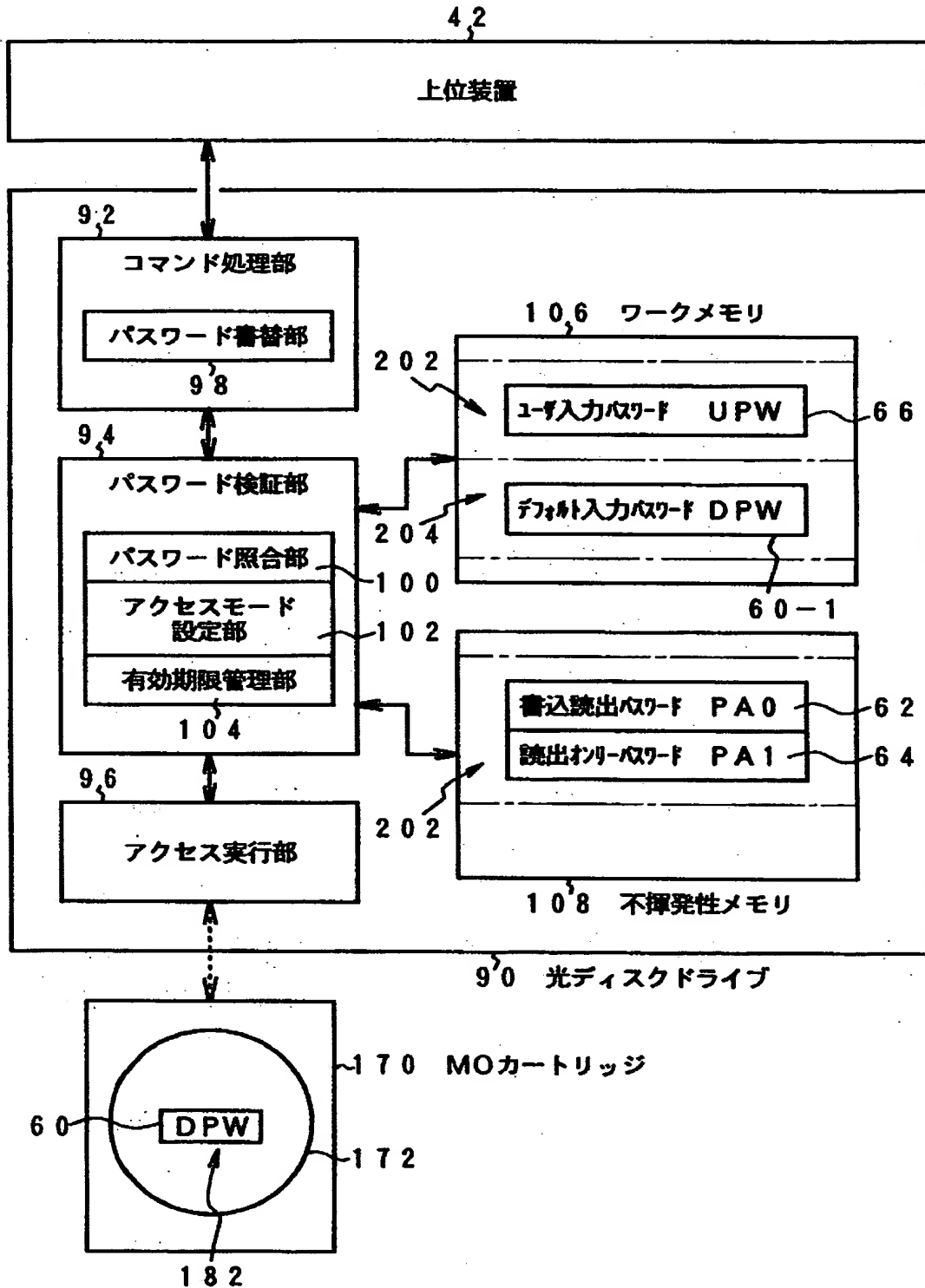
【図 21】

パスワードをMOドライブ本体とリムーバブル媒体に分けて保存した本発明の実施形態の機能ブロック図



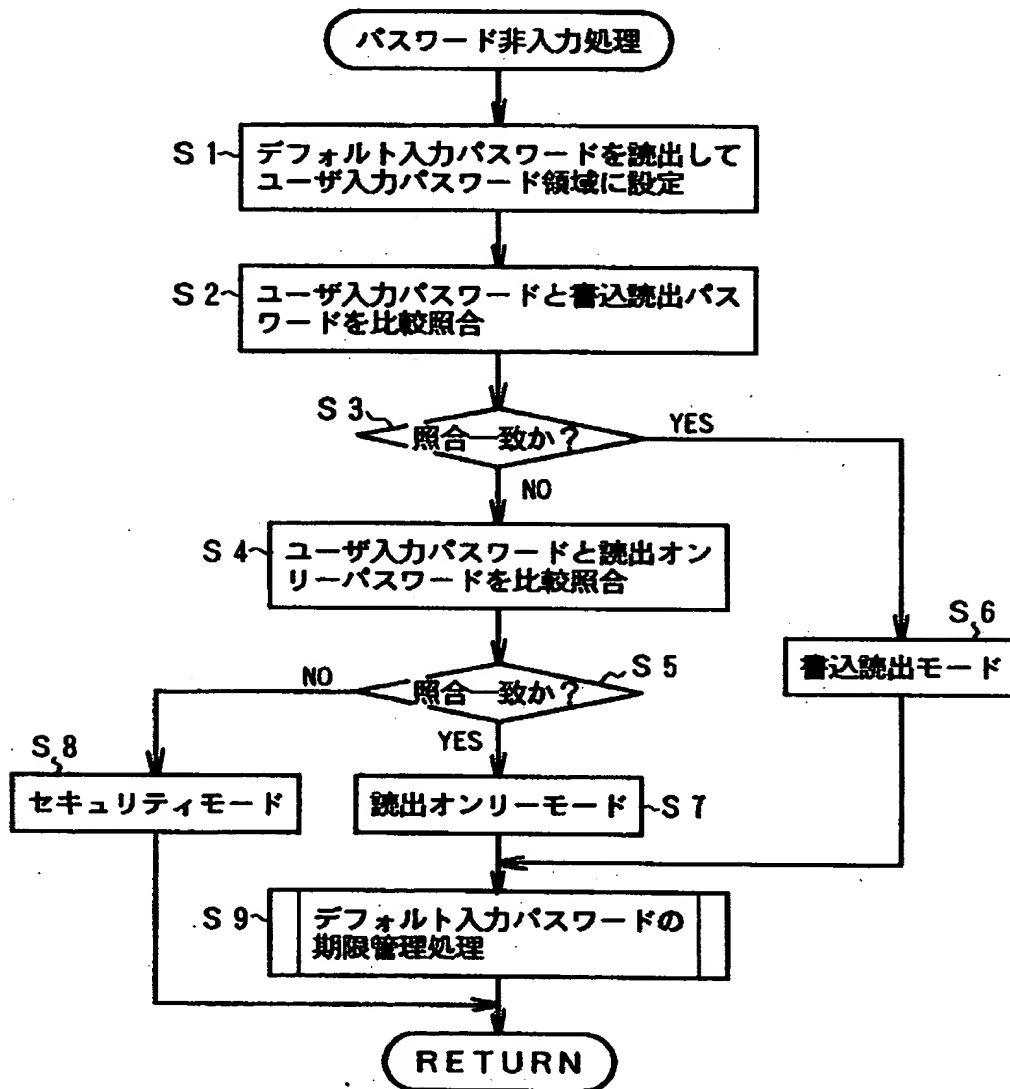
【図 22】

パスワードをMOドライブ本体とリムーバブル媒体に分けて保存した本発明の他の実施形態の機能ブロック図



【図 23】

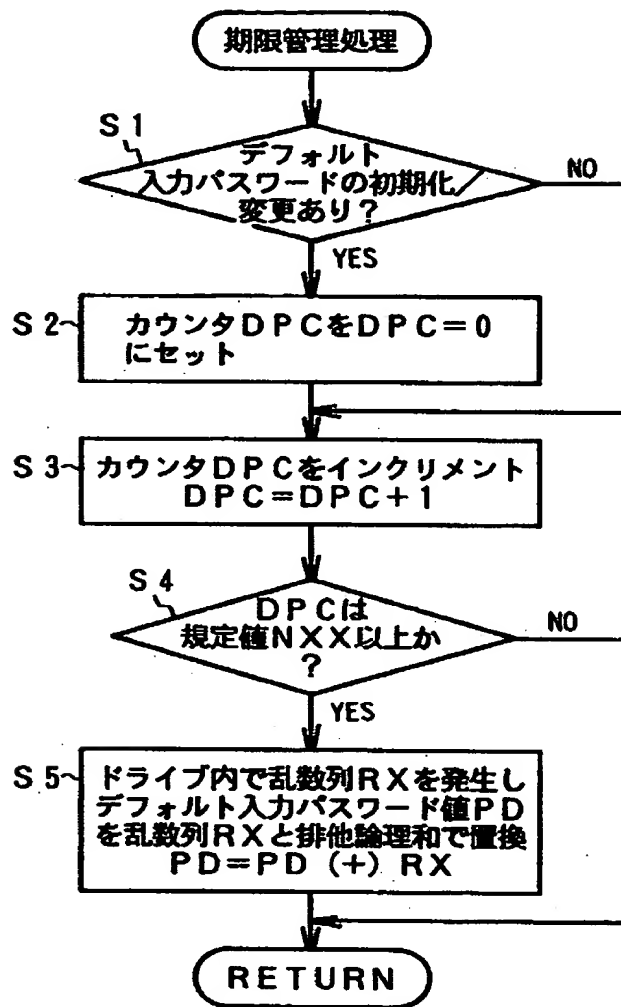
MOドライブにおけるユーザのパスワード入力がない場合のアクセス
保護処理のフローチャート



【図 2 4】

カウンタで使用回数を計数してデフォルト入力パスワードの期限を管理する

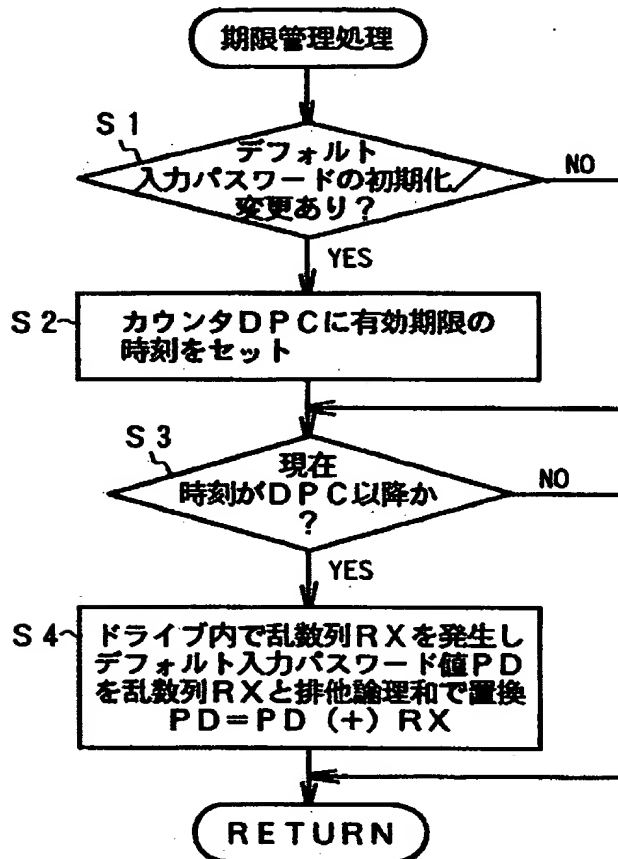
図 2 2 の有効期限管理処理のフローチャート



【図 25】

デフォルト入力パスワードの期限となる時刻を設定して管理する

図 22 の有効期限管理処理のフローチャート



【書類名】 要約書

【要約】

【課題】 パスワードによるアクセス保護を行っていても、ユーザのパスワード入力がなくともアクセスが許容され、パスワード入力の省略を可能とする。

【解決手段】 デフォルト入力パスワード60を保存し、ユーザからのパスワード入力がない場合はデフォルト入力パスワード60をユーザ入力パスワード66と見做してアクセス保護用パスワード62との比較照合によりアクセス保護を制御する。このときデフォルト入力パスワード60とアクセス保護用パスワード62が同じ値であれば照合一致となり、ユーザのパスワード入力を必要とすることなくアクセスが許可される。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号

【氏名又は名称】 富士通株式会社

【代理人】 申請人

【識別番号】 100079359

【住所又は居所】 東京都港区西新橋3丁目25番47号 清水ビル8
階

【氏名又は名称】 竹内 進

【選任した代理人】

【識別番号】 100093584

【住所又は居所】 東京都港区西新橋3丁目25番47号 清水ビル8
階

【氏名又は名称】 宮内 佐一郎

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社



Creation date: 10-30-2004
Indexing Officer: FNIGATU - FITSUM NIGATU
Team: OIPEBackFileIndexing
Dossier: 09159833

Legal Date: 06-05-2002

No.	Doccode	Number of pages
1	A...	1
2	SPEC	3
3	CLM	6
4	REM	12
5	XT/	1
6	IDS	1
7	LET.	1

Total number of pages: 25

Remarks:

Order of re-scan issued on